WTI Part No. 13532
Rev. D

RPC Series

Heavy Duty DC Network Power Switches

User's Guide

western™ telematic inc.

Warnings and Cautions:

Installation Instructions

Secure Racking

If Secure Racked units are installed in a closed or multi-unit rack assembly, they may require further evaluation by Certification Agencies. The following items must be considered.

1. The ambient within the rack may be greater than room ambient. Installation should be such that the amount of air flow required for safe operation is not compromised. The maximum temperature for the equipment in this environment is 55°C. Consideration should be given to the maximum rated ambient.
2. Installation should be such that a hazardous stability condition is not achieved due to uneven loading.
3. Side vents are used to dissipate heat generated within the unit. When mounting the unit in an equipment rack, make certain to allow adequate clearance for venting.

Input Supply

Check nameplate ratings to assure there is no overloading of supply circuits that could have an effect on overcurrent protection and supply wiring.

Grounding

Reliable earthing of this equipment must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than direct connections to the branch circuit.

No Serviceable Parts Inside; Authorized Service Personnel Only

Do not attempt to repair or service this device yourself. Internal components must be serviced by authorized personnel only.

- **Shock Hazard - Do Not Enter**
- **Lithium Battery**
  CAUTION: Danger of explosion if battery is incorrectly replaced. Replace only with same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Disconnect Power

If any of the following events are noted, immediately disconnect the unit from the outlet and contact qualified service personnel:

1. If the power cord becomes frayed or damaged.
2. If liquid has been spilled into the device or if the device has been exposed to rain or water.

Two Power Supplies

Note that this unit includes two separate power circuits. Before attempting to service or remove this unit, please make certain that both power sources are disconnected.

Table of Contents

1. Introduction 1-1

2. Unit Description. 2-1
   - 2.1. Front Panel Components - RPC-4850 Series 2-1
   - 2.2. Back Panel Components - RPC-4850 Series. 2-2
   - 2.3. Front Panel Components - RPC-40L8A4 Series 2-3
   - 2.4. Back Panel Components - RPC-40L8A4 Series 2-4
   - 2.5. Additional Button Functions 2-5

3. Getting Started 3-1
   - 3.1. Hardware Installation - RPC-4850 Series Units 3-1
     - 3.1.1. Apply Power to the RPC-4850 3-1
     - 3.1.2. Connect your PC to the RPC-4850 3-1
   - 3.2. Hardware Installation - RPC-40L8A4 Series Units 3-2
     - 3.2.1. Apply Power to the RPC-40L8A4 3-2
     - 3.2.2. Connecting Switched Devices to the RPC-40L8A4 3-3
     - 3.2.3. Output Terminal Fuses 3-4
     - 3.2.4. Connecting to the Alarm Inputs (RPC-40L8A4 Units Only) 3-5
   - 3.3. Communicating with the RPC Unit. 3-6

4. Hardware Overview. 4-1
   - 4.1. Applying Power to RPC-4850 Series Units 4-1
   - 4.2. Applying Power to RPC-40L8A4 Series Units 4-3
   - 4.3. Connecting Switched Devices to RPC-4850 Series Units 4-4
   - 4.4. Connecting Switched Devices to RPC-40L8A4 Series Units. 4-4
   - 4.5. Serial Console / RS232 Port Connection 4-4
     - 4.5.1. Connecting a Local PC. 4-4
     - 4.5.2. Connecting an External Modem. 4-4
   - 4.6. Connecting the Network Cable 4-5
   - 4.7. Output Terminal Fuses (RPC-40L8A4 Series Units Only) 4-5
   - 4.8. Connecting to the Alarm Inputs (RPC-40L8A4 Series Units Only) 4-5

5. Basic Configuration 5-1
   - 5.1. Communicating with the RPC Unit. 5-1
     - 5.1.1. The Text Interface 5-1
     - 5.1.2. The Web Browser Interface 5-3
     - 5.1.3. Access Via PDA 5-4
   - 5.2. Configuration Menus 5-5
   - 5.3. Defining System Parameters 5-6
     - 5.3.1. The Real Time Clock and Calendar 5-9
     - 5.3.2. The Invalid Access Lockout Feature 5-11
     - 5.3.3. Log Configuration 5-13
       - 5.3.3.1. Audit Log and Alarm Log Configuration Options. 5-14
       - 5.3.3.2. Reading, Downloading and Erasing Logs 5-14
     - 5.3.4. Callback Security 5-15
     - 5.3.5. Scripting Options 5-16
       - 5.3.5.1. Automated Mode 5-18
   - 5.4. User Accounts 5-19
     - 5.4.1. Command Access Levels. 5-19
     - 5.4.2. Circuit Access 5-20
     - 5.4.3. Port Access 5-20

5. Basic Configuration (continued)
5.5. Managing User Accounts . . . 5-21
5.5.1. Viewing User Accounts . . . 5-21
5.5.2. Adding User Accounts . . . 5-21
5.5.3. Modifying User Accounts . . . 5-24
5.5.4. Deleting User Accounts . . . 5-24
5.6. The Circuit Group Directory . . . 5-25
5.6.1. Viewing Circuit Groups . . . 5-25
5.6.2. Adding Circuit Groups . . . 5-26
5.6.3. Modifying Circuit Groups . . . 5-26
5.6.4. Deleting Circuit Groups . . . 5-26
5.7. Defining Circuit Parameters . . . 5-27
5.7.1. The Boot Priority Parameter . . . 5-28
5.7.1.1. Example 1: Change Circuit A3 to Priority 1 . . . 5-28
5.7.1.2. Example 2: Change Circuit A4 to Priority 2 . . . 5-29
5.8. Serial Port Configuration . . . 5-30
5.9. Network Configuration . . . 5-33
5.9.1. Network Port Parameters . . . 5-34
5.9.2. Network Parameters . . . 5-35
5.9.3. IP Security . . . 5-39
5.9.3.1. Adding IP Addresses to the Allow and Deny Lists . . . 5-40
5.9.3.2. Linux Operators and Wild Cards . . . 5-41
5.9.3.3. IP Security Examples . . . 5-41
5.9.4. Static Route . . . 5-42
5.9.5. Domain Name Server . . . 5-42
5.9.6. SNMP Access Parameters . . . 5-42
5.9.7. SNMP Trap Parameters . . . 5-44
5.9.8. LDAP Parameters . . . 5-45
5.9.8.1. Adding LDAP Groups . . . 5-47
5.9.8.2 Viewing LDAP Groups . . . 5-48
5.9.8.3. Modifying LDAP Groups . . . 5-48
5.9.8.4. Deleting LDAP Groups . . . 5-48
5.9.9. TACACS Parameters . . . 5-49
5.9.10. RADIUS Parameters . . . 5-51
5.9.10.1. Dictionary Support for RADIUS . . . 5-53
5.9.11. Email Messaging Parameters . . . 5-54
5.10. Save User Selected Parameters . . . 5-55
5.10.1. Restore Configuration . . . 5-55

6. Reboot Options . . . 6-1
6.1. Ping-No-Answer Reboot . . . 6-2
6.1.1. Adding Ping-No-Answer Reboots . . . 6-2
6.1.2. Viewing Ping-No-Answer Reboot Profiles . . . 6-4
6.1.3. Modifying Ping-No-Answer Reboot Profiles . . . 6-4
6.1.4. Deleting Ping-No-Answer Reboot Profiles . . . 6-4
6.2. Scheduled Reboot . . . 6-5
6.2.1. Adding Scheduled Reboots . . . 6-5
6.2.2. Viewing Scheduled Reboot Actions . . . 6-6
6.2.3. Modifying Scheduled Reboots . . . 6-6
6.2.4. Deleting Scheduled Reboots . . . 6-6

7. Alarm Configuration 7-1
7.1. The Over Temperature Alarms 7-2
7.1.1. Over Temperature Alarms - Load Shedding and Auto Recovery 7-4
7.2. The Circuit Breaker Open Alarm (RPC-40L8A4 Series Units Only) 7-6
7.3. The Lost Voltage (Line In) Alarm (RPC-40L8A4 Series Units Only) 7-8
7.4. The Ping-No-Answer Alarm 7-10
7.5. The Serial Port Invalid Access Lockout Alarm 7-12
7.6. The Power Cycle Alarm 7-14
7.7. The Alarm Input Alarm (RPC-40L8A4 Series Units Only) 7-15
7.8. The No Dialtone Alarm 7-17

8. The Status Screens 8-1
8.1. Product Status 8-1
8.2. The Network Status Screen 8-1
8.3. The Circuit Status Screen 8-2
8.4. The Circuit Group Status Screen 8-3
8.5. The Port Diagnostics Screen 8-3
8.6. Alias Status Screen 8-3
8.7. The Alarm Status Screen 8-4
8.8. The Serial Port Parameters Screen 8-4

9. Operation 9-1
9.1. Operation via the Web Browser Interface 9-1
9.1.1. The Circuit Control Screen - Web Browser Interface 9-1
9.1.2. The Circuit Group Control Screen - Web Browser Interface 9-2
9.2. Operation via the Text Interface 9-3
9.2.1. Switching and Reboot Commands - Text Interface 9-3
9.2.2. Applying Commands to Several Circuits - Text Interface 9-5
9.3. The Automated Mode 9-6
9.4. The SSH/Telnet Connect Function (Web Browser Interface Only) 9-7
9.4.1. Initiating an SSH Shell Session via the Web Browser Interface 9-7
9.4.2. Initiating a Telnet Session via the Web Browser Interface 9-8
9.5. Manual Operation 9-8
9.6. Logging Out of Command Mode 9-8

10. SSH Encryption 10-1

11. Syslog Messages 11-1
11.1. Configuration 11-1

12. SNMP Traps 12-1
12.1. Configuration 12-1

13. Operation via SNMP 13-1
13.1. RPC SNMP Agent 13-1
13.2. SNMPv3 Authentication and Encryption 13-1
13.3. Configuration via SNMP 13-2
13.3.1. Viewing Users 13-3
13.3.2. Adding Users 13-3
13.3.3. Modifying Users 13-3
13.3.4. Deleting Users 13-3
13.4. Circuit Control via SNMP 13-4
13.4.1. Circuit Status/Control 13-4
13.4.2. Circuit Group Status/Control 13-4
13.5. Viewing RPC Status via SNMP 13-5
13.5.1. System Status - Ethernet Port Mac Addresses 13-5
13.5.2. Circuit Status 13-5
13.5.3. Unit Environment Status 13-5
13.5.4. Alarm Status 13-6
13.6. Sending Traps via SNMP 13-7

14. Setting Up SSL Encryption 14-1
14.1. Creating a Self Signed Certificate 14-2
14.2. Creating a Signed Certificate 14-3
14.3. Downloading the Server Private Key 14-4
14.4. TLS Mode 14-5

15. Saving and Restoring Configuration Parameters 15-1
15.1. Sending Parameters to a File 15-1
15.1.1. Downloading & Saving Parameters via Text Interface 15-1
15.1.2. Downloading & Saving Parameters via Web Browser Interface 15-2
15.2. Restoring Saved Parameters 15-2
15.3. Restoring Previously Saved Parameters 15-3

16. Upgrading RPC Firmware 16-1
16.1. WMU Enterprise Management Software (Recommended) 16-1
16.2. The Upgrade Firmware Function (Alternate Method) 16-1

17. Command Reference Guide 17-1
17.1. Command Conventions 17-1
17.2. Command Summary 17-2
17.3. Command Set 17-3
17.3.1. Display Commands 17-3
17.3.2. Control Commands 17-6
17.3.3. Configuration Commands 17-11

Appendices:

A. Specifications Apx-1
A.1. RPC-4850 Series Units Apx-1
A.2. RPC-40L8A4 Series Units Apx-2

B. Interface Descriptions Apx-3
B.1. RS232 Console Port - RPC-4850 Series Units Apx-3
B.2. RS232 Console Port - RPC-40L8A4 Series Units Apx-3

C. Customer Service Apx-4

List of Figures

2.1. Front Panel (Model RPC-4850-48V Shown) 2-1
2.2. Back Panel (Model RPC-4850-48V Shown) 2-2
2.3. Front Panel (Model RPC-40L8A4 Shown). 2-3
2.4. Back Panel (Model RPC-40L8A4 Shown). 2-4
3.1. DC Input Block Terminal (RPC-40L8A4 Series - Protective Cover Not Shown) 3-2
3.2. DC Output Terminal Blocks (RPC-40L8A4 Series - Fuses Not Shown) 3-3
3.3. DC Output Terminal Block Fuses (RPC-40L8A4 Series Units Only). 3-4
3.4. Connecting to the Alarm Inputs (RPC-40L8A4 Series Units Only). 3-5
4.1. Model RPC-4850 Series Block Diagram (Model RPC-4850-48V Shown) 4-2
4.2. RPC-40L8A4 Series Units; Block Diagram 4-3
5.1. Boot Priority Example 1. 5-28
5.2. Boot Priority Example 2. 5-29
14.1. Web Access Parameters (Text Interface Only) 14-1
B.1. RS232 Console Port Interface - RPC-4850 Series Units. Apx-3
B.2. RS232 Console Port Interface - RPC-40L8A4 Series Units Apx-3

1. Introduction

Electronic equipment sometimes "locks-up," requiring a service call just to flip the power switch to perform a simple reboot. RPC Series Heavy Duty Remote DC Power Controllers give you the ability to perform this function from anywhere, just point your browser to the RPC's IP address, enter the secure password, and you're just a click away from remote power and reboot control!

Intelligent Power Control

The RPC can be configured and operated via local console port, Telnet, Web, SSL, SSH or SNMP. In situations where a network connection is unavailable, users can also establish and out of band connection with the RPC using an external modem and basic VT100 type terminal emulation.

Security and Co-Location Features:

Secure Shell (SSHv2) encryption and address-specific IP security masks help to prevent unauthorized access to command and configuration functions.

The RPC provides four different levels of security for user accounts: Administrator, SuperUser, User and ViewOnly. The Administrator level provides complete access to all circuit control functions, operating features and configuration menus. The SuperUser level allows switching and rebooting of all circuits but does not allow access to configuration functions. The User level allows access to only a select group of Administrator-defined circuits. The ViewOnly level allows you to check circuit status and unit status, but does not allow switching or rebooting of circuits or access to configuration menus.

The RPC is compatible with popular remote authentication protocols such as LDAP, Kerberos, TACACS+ and Radius. In addition, the RPC also supports MIB commands, and operation and configuration via SNMP.

Easy to Configure, Easy to Use

The RPC can be configured via network, modem, or locally via serial Console Port. Simple, user-friendly commands are employed to assign configuration parameters, enable alarm features and view unit status. Circuits can be switched On, Off, or rebooted using simple ASCII commands or user-friendly Web based menus.

RPC Series Models:

This user's guide covers several different RPC models. Specifications for the models covered in this user's guide are summarized in the table below:

Model No.	Input Feeds	Input Voltage	Max. Load per Outlet	Max. Load per Input	Max. Load per Unit
RPC-4850-48V	2 ea, 50 Amp Redundant	-18 to -72 VDC	15 Amps	50 Amps	50 Amps
RPC-4850-24V	2 ea, 50 Amp Redundant	18 to 72 VDC	15 Amps	50 Amps	50 Amps
RPC-40L8A4-48	2 ea, 40 Amp	18 to 72 VDC	10 Amps	40 Amps	2 @ 40 Amps ea.
RPC-40L8A4-24	2 ea, 40 Amp	18 to 72 VDC	10 Amps	40 Amps	2 @ 40 Amps ea.
RPC-40L8A4-12	2 ea, 40 Amp	9 to 36 VDC	10 Amps	40 Amps	2 @ 40 Amps ea.

Note that througout this user's guide, the various RPC models are referred to as follows:

- **RPC** or **RPC Series** - All RPC Models
- **RPC-4850 Series** - Models RPC-4850-48V and RPC-4850-24V
- **RPC-40L8A4 Series** - Models RPC-40L8A4-48, RPC-40L8A4-24 and RPC-40L8A4-12

Typographic Conventions

^ (e.g. **^X**)	Indicates a control character. For example, the text "**^X**" (Control X) indicates **[Ctrl]** and **[X]** key must be pressed at the same time.
`COURIER FONT`	Indicates characters typed on the keyboard. For example, **`/AC`** or **`/ON A2`**.
[Bold Font]	Text set in bold face and enclosed in square brackets indicates a specific key. For example, **[Enter]** or **[Esc]**.
< >	Indicates required keyboard entries. For Example: **`/P <n>`**.
[ ]	Indicates optional keyboard entries. For Example: **`/P [n]`**.

2. Unit Description

2.1. Front Panel Components - RPC-4850 Series

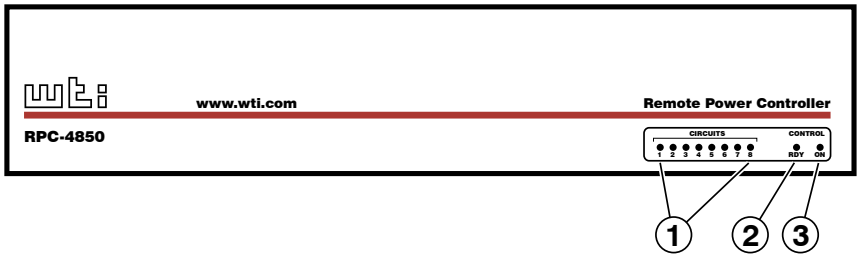

Figure 2.1: Front Panel (Model RPC-4850-48V Shown)

As shown in Figure 2.1, the RPC-4850 Series Front Panel includes the following:

① **Circuit Status Indicators:** A series of eight LED indicators, which light when power to the corresponding circuit is Switched On.

② **RDY Indicator:** Flashes when the RPC is ready to receive commands.

③ **ON Indicator:** Lights when power is applied to the Control Section.

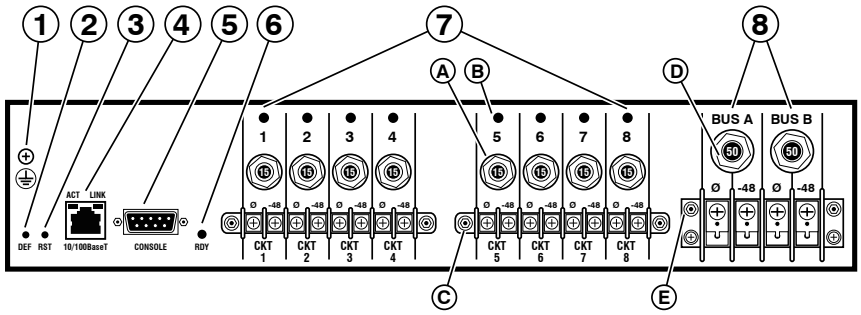

Figure 2.2: Back Panel (Model RPC-4850-48V Shown)

2.2. Back Panel Components - RPC-4850 Series

As shown in Figure 2.2, the RPC-4850 Series back panel includes the following:

> **Note:** *All Reset and Default button functions can also be disabled via the System Parameters menu, as described in Section 5.3.*

① **Ground Screw**

② **Default Button:** Toggles circuits On/Off or resets unit to factory default parameters as described in Section 2.5.

③ **Reset Button:** Reboots and/or resets the RPC to factory defaults as described in Section 2.5.

④ **Network Port:** An RJ45 Ethernet port for connection to your 10/100Base-T, TCP/IP network. Note that the RPC features a default IP address (192.168.168.168). This allows you to connect to the unit without first assigning an IP address. Note that the Network Port also includes two, small LED indicators for Link and Data Activity. For more information on Network Port configuration, please refer to Section 5.9.

⑤ **Console Port:** A DB9, RS232 serial port (DTE), for connection to a local terminal or external modem, as described in Section 4.5.

⑥ **RDY Indicator:** (Ready) Flashes to indicate that unit is ready to receive commands.

⑦ **Switched Output Circuits:** A series of eight DC, 15 Amp circuits divided into two terminal blocks.

A. **15 Amp Circuit Breakers:** Each circuit includes a 15 Amp breaker.

B. **Status Indicators:** Each circuit includes a Status Indicator, which lights when the circuit is switched On.

C. **Mounting Screw Receptacles:** Each terminal block includes two mounting screw receptacles, which are used to install the protective cover (not shown.)

⑧ **Power Input:** Two DC input Buses.

D. **50 Amp Circuit Breakers:** Each power input bus includes a 50 Amp breaker.

E. **Mounting Screw Receptacles:** The power input terminal block includes two mounting screw receptacles, which are used to install the protective cover (not shown).

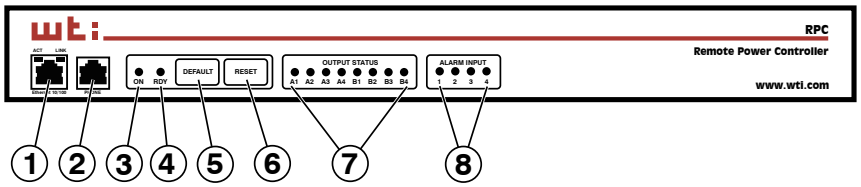

Figure 2.3: Front Panel (Model RPC-40L8A4 Shown)

2.3. Front Panel Components - RPC-40L8A4 Series

As shown in Figure 2.3, the RPC-40L8A4 Series Front Panel includes the following:

> **Note:** *All Reset and Default button functions can also be disabled via the System Parameters menu, as described in Section 5.3.*

① **Network Port:** An RJ45 Ethernet port for connection to your 10/100Base-T, TCP/IP network. Note that the RPC features a default IP address (192.168.168.168). This allows you to connect to the unit without first assigning an IP address. Note that the Network Port also includes two, small LED indicators for Link and Data Activity. For more information on Network Port configuration, please refer to Section 5.9.

② **Console Port:** A DB9, RS232 serial port (DTE), for connection to a local terminal or external modem, as described in Section 4.5.

③ **ON Indicator:** Lights when power is applied to the Control Section.

④ **RDY Indicator:** Flashes when the RPC is ready to receive commands.

⑤ **Default Button:** Toggles circuits On/Off or resets unit to factory default parameters as described in Section 2.5.

⑥ **Reset Button:** Reboots and/or resets the RPC to factory defaults as described in Section 2.5.

⑦ **Circuit Status Indicators:** A series of eight LED indicators, which light when power to the corresponding circuit is Switched On.

⑧ **Alarm Input Indicators:** A series of four LED indicators which light when the corresponding Alarm Input has generated an alarm. For more information on Alarm Input functions, please refer to Section 7.7.

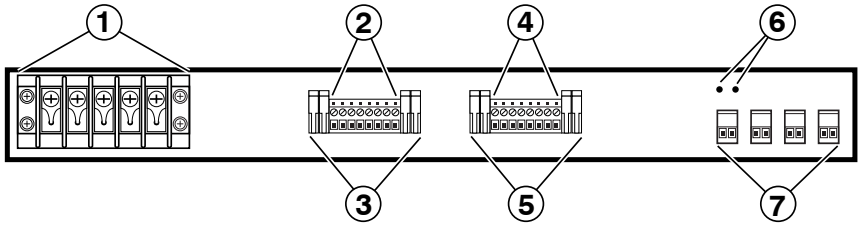

Figure 2.4: Back Panel (Model RPC-40L8A4 Shown)

2.4. Back Panel Components - RPC-40L8A4 Series

As shown in Figure 2.4, the RPC-40L8A4 Series Back Panel includes the following:

① **Power Input:** Two 40 Amp DC input Buses that share a common chassis ground line. The power input terminal block also includes two mounting brackets, which are used to hold the protective cover (not shown).

② **Switched Output Circuits - Bus A:** Four ten amp DC circuits in a Euro Style output terminal fed by power input bus A. DC output voltages for RPC-40L8A4 series units are as follows:

- RPC-40L8A4-48 = ± 48 V DC, 10 Amps
- RPC-40L8A4-24 = + 24 V DC, 10 Amps
- RPC-40L8A4-12 = + 12 V DC, 10 Amps

③ **Output Circuit Fuses - Bus A:** Four ten amp DC GMT fuses that protect the circuits on Output Bus A. Ships with 10 Amp fuses; for custom fuses, please contact WTI

④ **Switched Output Circuits - Bus B:** Four ten amp DC circuits in a Euro Style output terminal fed by power input bus B. Voltages for each RPC-40L8A4 model are described under item 2 above.

⑤ **Output Circuit Fuses - Bus B:** Four ten amp DC GMT fuses that protect the circuits on Output Bus B. Ships with 10 Amp fuses; for custom fuses, please contact WTI

⑥ **Optional Grounding Lug Location:** Mounting holes for optional grounding lug for 6 gauge ground wire. For more information, please contact WTI.

⑦ **Alarm Inputs:** Four Euro style alarm inputs, which are designed for connection to door open alarms or other dry contacts. Each alarm input supplies 0.4 Amps of positive DC current at the same voltage that is used to power the unit (e.g., ± 48 V DC units provide +48 V DC, +24 V DC units provide +24 V DC and +12 V DC units provide +12 V DC.)

2.5. Additional Button Functions

The Default and Reset buttons can be used to perform the functions described below:

Notes:

- *All button functions can also be disabled via the System Parameters menu, as described in Section 5.3.*
- *When the RPC is reset to factory defaults, all user-defined configuration parameters will be cleared, and the default "super" user account will also be restored.*

1. **Reboot Operating System:**
   a) Press and hold the Reset button for five seconds, and then release it.
   b) The RPC will reboot it's operating system; all circuits will be left in their current On/Off state.
2. **Set Parameters to Factory Defaults:**
   a) Simultaneously press both the Default button and the Reset button, hold them for five seconds, and then release them.
   b) All RPC parameters will be reset to their original factory default settings, and the unit will then reboot. All circuits will be left in their current On/Off state.
3. **Toggle/Default All Circuits:**
   a) Press the Default button, hold it for five seconds, and then release the Default Button.
   b) The RPC will switch all circuits to the Off state. If all circuits are already in the Off state, then the unit will reset all circuits to their user defined default states.

3. Getting Started

This Quick Start Guide describes a simplified installation procedure for the RPC, which will allow you to communicate with the unit in order to demonstrate basic features and check for proper operation.

Notes:

- *There are separate Hardware Installation procedures for RPC-4850 series units and RPC-40L8A4 series units. RPC-4850 series units are discussed in Section 3.1 and RPC-40L8A4 series units are discussed in Section 3.2.*
- *This Quick Start Guide does not describe unit configuration or discuss advanced operating features in detail. For more information, please refer to the remainder of this User's Guide.*

3.1. Hardware Installation - RPC-4850 Series Units

3.1.1. Apply Power to the RPC-4850

Refer to power rating nameplate on the back panel, and then connect the RPC-4850 series unit to an appropriate power source as shown in Figure 4.1.

The RPC-4850 features two separate DC inputs; connect power wires to the unit's Circuit "A" and/or Circuit "B" terminal blocks, then connect the wires to an appropriate power supply. Note that it is not necessary to connect power to both input circuits; either circuit will supply power for operation and control functions. However, when power is connected to both circuits, this allows the second circuit to function as a back-up in the event of a power outage. The ON LED should light, and the RDY LED should begin to flash. This indicates that the RPC-4850 is ready to receive commands.

Note that each individual output circuit will support up to 15 Amps maximum, and that the total for all eight circuits cannot exceed 50 Amps.

3.1.2. Connect your PC to the RPC-4850

The RPC can either be controlled by a local PC, that communicates with the unit via cable, controlled via external modem, or controlled via TCP/IP network. Note that it is not necessary to connect to both the Network and Console Ports, and that the Console Port can be connected to either a local PC or External Modem.

- **Network Port:** Connect your 10Base-T or 100Base-T network interface to the RPC Network port.
- **Console Port:** Use the null modem cable supplied with the unit to connect your PC COM port to the RPC Console (RS232) Port.
- **External Modem:** Use a standard AT or modem cable to connect your external modem to the RPC's Console (RS232) Port.

3.2. Hardware Installation - RPC-40L8A4 Series Units

3.2.1. Apply Power to the RPC-40L8A4

Refer to power rating nameplate on the back panel, and then remove the protective cover from the terminal block and connect the RPC-40L8A4 unit to an appropriate power source as shown in Figure 3.1 below.

Note: *RPC-40L8A4 series units feature two completely independent buses, and for each circuit, voltage is connected to the +/- terminal (for negative 48 or positive 48 volt units, power is connected to the +/- terminals and for positive 24 and 12 volt units, positive power is also connected to the +/- terminals.)*

Warning: ***An exposed wire lead from a DC input power source can conduct harmful levels of electricity. Make certain that no exposed portion of the DC input wire extends from the terminal block.***

Input voltages for RPC-40L8A4 units are described in the table below:

Model Number	Voltage	Voltage Range
RPC-40L8A4-48	+48 or - 48 VDC	18 to 72 VDC
RPC-40L8A4-24	+24 VDC	18 to 72 VDC
RPC-40L8A4-12	+12 VDC	9 to 36 VDC

When you have finished connecting power lines to the RPC-40L8A4 unit, make certain to replace the protective input terminal block cover.

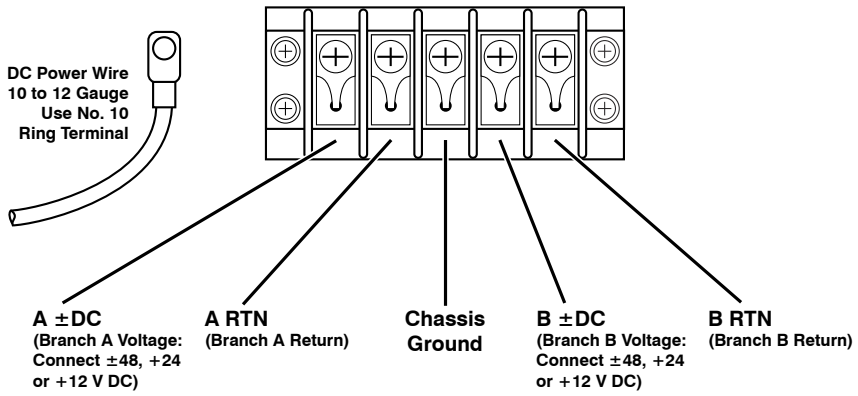

Figure 3.1: DC Input Block Terminal (RPC-40L8A4 Series - Protective Cover Not Shown)

3.2.2. Connecting Switched Devices to the RPC-40L8A4

The output terminals on the RPC-40L8A4 back panel are used to connect DC voltage to each switched device. Each output terminal includes eight connectors (four circuits.) To connect wires to the DC output terminal block, refer to Figure 3.2 below and proceed as follows:

Note: *Each individual output circuit will support up to 10 Amps maximum; the total for all four circuits on either bus cannot exceed 40 Amps.*

Warning: ***An exposed wire lead from a DC input power source can conduct harmful levels of electricity. Make certain that no exposed portion of the DC input wire extends from the terminal block.***

1. Firmly insert the wire into the wire hole and push the wire into the hole until resistance is felt.

2. While holding the wire in place, use a screwdriver with a 3mm wide blade to tighten the retaining screw; the screwdriver that is used to tighten the retaining screw must be narrow enough to reach the retaining screw unobstructed. Note that in order to properly secure the wire, you must push down on the screwdriver while tightening the retaining screw until the screw is firmly seated.

   Note: *If you have difficulty securing the wire to the terminal block, make certain that you are using a screwdriver with a 3 mm wide blade (or narrower,) and that the retaining screw and is tight enough to hold the wire in place.*

   Caution: ***Do not over tighten the retaining screws. The recommended maximum torque is 4.5 lbf-in (72 ozf-in.)***

3. Tug on the wire to make certain that the wire is firmly held in place.

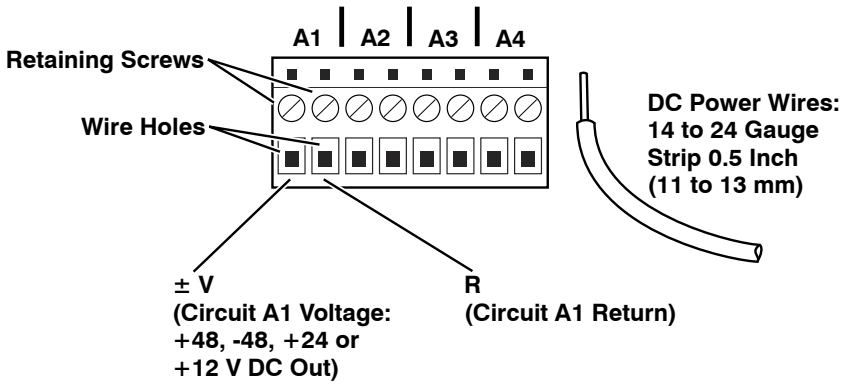

Figure 3.2: DC Output Terminal Blocks (RPC-40L8A4 Series - Fuses Not Shown)

3.2.3. Output Terminal Fuses

Note that each output terminal includes four fuses; one for each circuit on the output terminal. If a fuse is blown, a red dot will appear in the clear cap as shown in Figure 3.3. To remove a fuse, use a pair of pliers to grasp the black body of the fuse, and then gently pull the fuse loose from the RPC-40L8A4 unit. The RPC-40L8A4 ships with 10 Amp fuses; for custom fuses, please contact WTI.

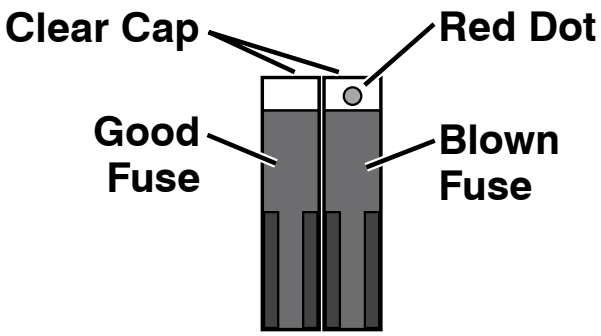

Figure 3.3: DC Output Terminal Block Fuses (RPC-40L8A4 Series Units Only)

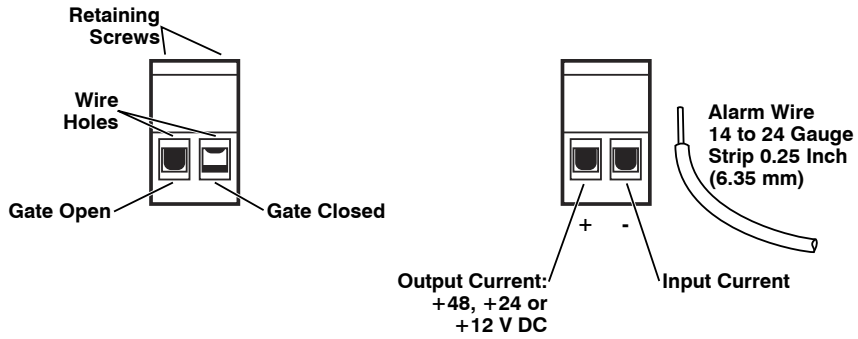

Figure 3.4: Connecting to the Alarm Inputs (RPC-40L8A4 Series Units Only)

3.2.4. Connecting to the Alarm Inputs (RPC-40L8A4 Units Only)

The RPC-40L8A4 back panel includes four alarm inputs, designed for connection to door open alarms or other dry contact alarms. Each + pin supplies positive DC voltage at the same voltage that is used to power the unit (i.e., ± 48 V DC units provide +48 V DC, +24 V DC units provide +24 V DC and +12 V DC units provide +12 V DC.)

Note that when the RPC-40L8A4 unit is shipped from the factory, the removable alarm input connectors are enclosed in separate plastic bag, included in the shipping box and must be installed by the user.

When connecting wires to alarm inputs, make certain each wire is properly seated and firmly held in place by the retaining screw. As shown in Figure 3.4, in order to properly seat the wire the retaining screw must be turned counter-clockwise until the metal "gate" in the wire hole is open. If the metal gate is closed, the wire will not seat properly. After inserting the wires, tighten both screws to secure the wires to the connector and snap the connector in place on the back panel of the RPC-40L8A4 unit.

> **Caution:** ***Do not over tighten the retaining screws. The recommended maximum torque is 4.5 lbf-in (72 ozf-in.)***

3.3. Communicating with the RPC Unit

In order to ensure security, both Telnet and Web Browser Access are disabled when the RPC is shipped from the factory. To enable Telnet and/or Web Browser access, please refer to Section 5.9.2. When properly installed and configured, the RPC can allow command mode access via Telnet, Web Browser, SSH client, modem, or local PC.

Notes:

- *Default RPC serial port parameters are set as follows: 9600 bps, RTS/CTS Handshaking, 8 Data Bits, One Stop Bit, No Parity. Although these parameters can be easily redefined, for this Quick Start procedure, it is recommended to configure your communications program to accept the default parameters.*
- *The RPC features a default IP Address (192.168.168.168) and a default Subnet Mask (255.255.255.0.) This allows network access to command mode, providing that you are contacting the RPC from a node on the same subnet. When attempting to access the RPC from a node that is not on the same subnet, please refer to the User's Guide for further configuration instructions.*

1. **Access Command Mode:** The RPC includes two separate user interfaces; the Text Interface and the Web Browser Interface. The Text Interface is available via Local PC, SSH Client, Telnet, or Modem. The Web Browser interface is only available via TCP/IP network.

   a) **Via Local PC:** Start your communications program and then press **[Enter]**.

   b) **Via SSH Client:** Start your SSH client, enter the default IPv4 format IP address (192.168.168.168) for the RPC and invoke the connect command.

   c) **Via Web Browser:** Make certain that Web Browser access is enabled as described in the RPC User's Guide. Start your JavaScript enabled Web Browser, enter the default IPv4 format IP address (192.168.168.168) in the Web Browser address bar, and then press **[Enter]**.

   d) **Via Telnet:** Make certain that Telnet access is enabled as described in the RPC User's Guide. Start your Telnet client, and enter the default IPv4 format IP address (192.168.168.168).

   e) **Via Modem:** Make certain that the RPC Console Port has been configured for Modem Mode as described in the RPC User's Guide, then use your communications program to dial the number for the external Modem connected to the Console Port.

2. **Username** / **Password Prompt:** A message will be displayed, which prompts you to enter your username and password. The default username is "super" (all lower case, no quotes), and the default password is also "super". If a valid username and password are entered, the RPC will display either the Circuit Control Screen (Web Browser Interface) or the Circuit Status Screen (SSH, Telnet, or Modem).

3. **Test Switching Functions:** You may wish to perform the following tests in order to make certain that the RPC is responding to commands. When switching and reboot commands are executed, the Status LED(s) will also turn On or Off to indicate the current status of the circuit(s).

   a) **Reboot Circuit:**

      i. **Web Browser Interface:** Click on the "Circuit Control" link on the left hand side of the screen to display the Circuit Control Menu. From the Circuit Control Menu, click the down arrow in the row for Circuit 1 to display the dropdown menu, then select "Reboot" from the drop down menu and click on the "Execute Actions" button.

      ii. **Text Interface:** Type **`/BOOT 1`** and press **[Enter]**.

   b) **Switch Circuit Off:**

      i. **Web Browser Interface:** From the Circuit Control Menu, click the down arrow in the "Action" column for Circuit 1 to display the drop down menu, then select "Off" from the drop down menu and click on the "Execute Actions" button.

      ii. **Text Interface:** Type **`/OFF 1`** and press **[Enter]**.

   c) **Switch Circuit On:**

      i. **Web Browser Interface:** From the Circuit Control Menu, click the down arrow in the "Action" column for Circuit 1 to display the drop down menu, then select "On" from the drop down menu and click on the "Execute Actions" button.

      ii. **Text Interface:** Type **`/ON A1`** and press **[Enter]**.

This completes the Quick Start Guide for the RPC. Prior to placing the unit into operation, it is recommended to refer to the remainder of this User's Guide for important information regarding advanced configuration capabilities and more detailed operation instructions. If you have further questions regarding the RPC unit, please contact WTI Customer Support as described in Appendix C.

4. Hardware Overview

4.1. Applying Power to RPC-4850 Series Units

Note: *This procedure differs for RPC-40L8A4 series units. For instructions on connecting power to RPC-40L8A4 series units, please refer to Section 4.2.*

Refer to power rating nameplate on the back panel, and then connect the RPC-4850 series unit to an appropriate power source as shown in Figure 4.1.

RPC-4850 series units features two separate DC inputs; connect power cables to the unit's Circuit "A" and/or Circuit "B" terminal blocks, then connect the cables to an appropriate power supply. Note that it is not necessary to connect power to both input circuits; either circuit will supply power for operation and control functions. However, when power is connected to both circuits, this allows the second circuit to function as a back-up in the event of a power outage.

Note that each individual output circuit will support up to 15 Amps maximum, and that the total for all eight circuits cannot exceed 50 Amps.

CAUTIONS:

- ***Before attempting to install this unit, please review the warnings and cautions listed at the front of the user's guide.***
- ***This device should only be operated with the type of power source indicated on the instrument nameplate. If you are not sure of the type of power service available, please contact your local power company.***
- ***Reliable earthing (grounding) of this unit must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than directly to the branch circuit.***

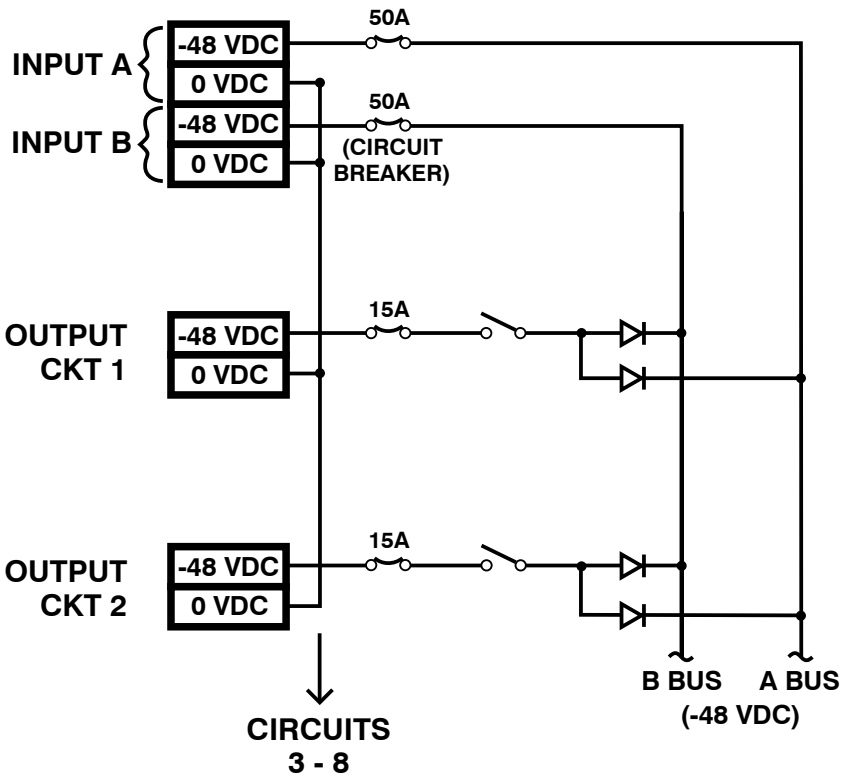

Figure 4.1: Model RPC-4850 Series Block Diagram (Model RPC-4850-48V Shown)

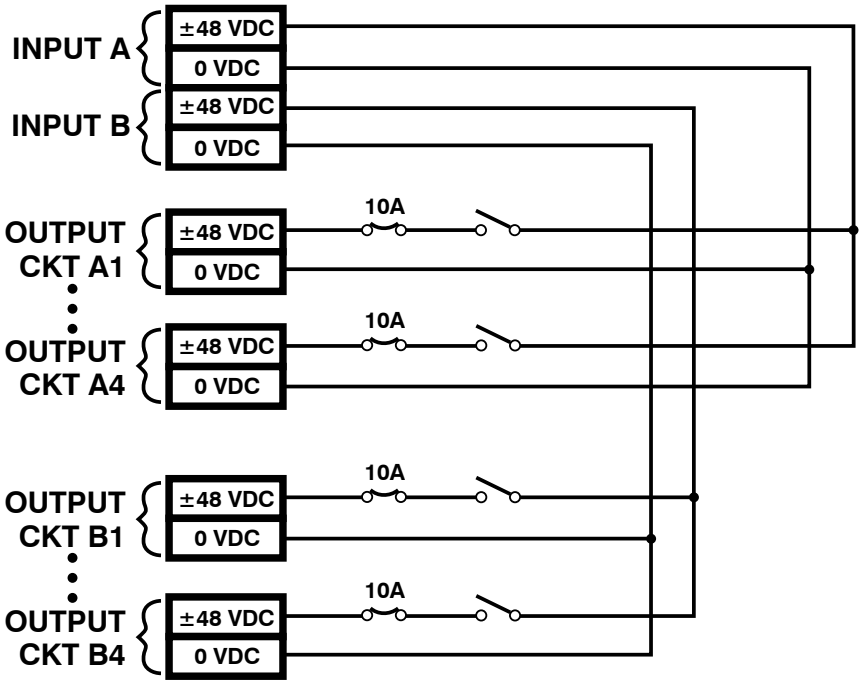

Figure 4.2: RPC-40L8A4 Series Units; Block Diagram

4.2. Applying Power to RPC-40L8A4 Series Units

Note: *This procedure differs for RPC-4850 series units. For instructions on connecting power to RPC-4850 series units, please refer to Section 4.1.*

Refer to power rating nameplate on the back panel, and then connect the RPC-40L8A4 series unit to an appropriate power source as shown in Figure 4.2. For further details regarding power connection to RPC-40L8A4 series units, please refer to Section 3.2.1 in this user's guide.

4.3. Connecting Switched Devices to RPC-4850 Series Units

> **Note:** *This procedure differs for RPC-40L8A4 series units. For instructions on connecting switched devices to RPC-40L8A4 series units, please refer to Section 4.4.*

Make certain that the power supply to the RPC-4850 series unit is switched Off, and then connect the supply cables from your DC powered devices to the Switched Output Circuits on the RPC-4850 back panel. Check to make certain that cables are securely attached, and then install the protective covers over each output terminal block. The protective covers are held in place by screws that pass through the holes in the cover and then thread into the screw receptacles at the end of each Output Terminal Block.

4.4. Connecting Switched Devices to RPC-40L8A4 Series Units

> **Note:** *This procedure differs for RPC-4850 series units. For instructions on connecting switched devices to RPC-4850 series units, please refer to Section 4.3.*

The output terminals on the RPC-40L8A4 back panel are used to connect DC voltage to each switched device. Each output terminal includes eight connectors (four circuits.) For further details regarding connecting switched devices to RPC-40L8A4 series units, please refer to Section 3.2.2 in this user's guide.

4.5. Serial Console / RS232 Port Connection

The Serial Console Port can be connected to either an external modem or a local PC, but not both items at the same time. In the default state, the Console port is configured for 9600 bps, no parity, 8 data bits, 1 stop bit. Appendix B describes the Console Port interface. Note that RPC-4850 series units differ from RPC-40L8A4 series units as follows:

- **RPC-4850 Series Units:** The RPC-4850 Console Port is a male, RS232C DB9 connector.
- **RPC-40L8A4 Series Units:** The RPC-40L8A4 Console Port is a female RS232C RJ45 connector.

4.5.1. Connecting a Local PC

Use the supplied null modem cable to connect your PC Console port to the RPC Console (RS232) Port. Make certain that the Serial Port Mode is set to "Normal" as described in Section 5.8.

4.5.2. Connecting an External Modem

When connecting directly to an external modem, use a standard AT to Modem cable. Make certain that the modem is initialized at the same default parameters as the RPC Console Port. Make certain that the RPC Serial Port Mode is set to "Modem" as described in Section 5.8.

4.6. Connecting the Network Cable

The Network Port is an RJ45 Ethernet jack, for connection to a TCP/IP network. Connect your 10Base-T cable to the Network Port. Note that the RPC includes a default IP address (192.168.168.168) and a default subnet mask (255.255.255.0.) When installing the RPC in a working network environment, it is recommended to define network parameters as described in Section 5.9.

> **Note:** *The RPC features a 10/100Base-T auto-negotiating Interface; speed and duplex mode will be automatically negotiated. When connecting to a 100Base-T interface, most router switches will autosense to determine if the device is 100Base-T or 10Base-T, and then configure the network interface accordingly. If your router switch does not autosense, the RPC will auto negotiate speed and duplex mode.*

4.7. Output Terminal Fuses (RPC-40L8A4 Series Units Only)

On RPC-40L8A4 series units, each output terminal includes four fuses; one for each circuit on the output terminal. For further details regarding detecting blown fuses and changing fuses, please refer to Section 3.2.3 in this user's guide.

4.8. Connecting to the Alarm Inputs (RPC-40L8A4 Series Units Only)

The RPC-40L8A4 back panel includes four alarm inputs, designed for connection to door open alarms or other dry contact alarms. For further details regarding connecting devices to the Alarm Inputs, please refer to Section 3.2.4 in this user's guide.

This completes the RPC installation instructions. Please proceed to Section 5 for instructions regarding unit configuration.

5. Basic Configuration

This section describes the basic configuration procedure for all RPC units. For more information on Reboot Options and Alarm Configuration, please refer to Section 6 and Section 7.

5.1. Communicating with the RPC Unit

In order to configure the RPC, you must first connect to the unit, and access command mode. Note that, the RPC offers two separate configuration interfaces; the Web Browser Interface and the Text Interface.

In addition, the RPC also offers three different methods for accessing command mode; via network, via external modem, or via local console. The Web Browser interface is only available via network, and the Text Interface is available via network (SSH or Telnet), modem or local PC.

5.1.1. The Text Interface

The Text Interface consists of a series of simple ASCII text menus, which allow you to set options and define parameters by entering the number for the desired option using your keyboard, and then typing in the value for that option.

Since the Web Browser Interface and Telnet accessibility are both disabled in the default state, you will need to use the Text Interface to contact the RPC via Local PC or SSH connection when setting up the unit for the first time. After you have accessed command mode using the Text Interface, you can then enable Web Access and Telnet Access, if desired, in order to allow future communication with the unit via Web Browser or Telnet. You will not be able to contact the unit via Web Browser or Telnet until you have enabled these options.

Once Telnet Access is enabled, you will then be able to use the Text Interface to communicate with the RPC via local PC, Telnet or SSH connection. You can also use the Text Interface to access command mode via an external modem installed at the RPC serial Console Port.

In order to use the Text Interface, your installation must include:

- **Access via Network:** The RPC must be connected to your TCP/IP Network, and your PC must include a communications program (such as HyperTerminal.)
- **Access via Modem:** An external modem must be installed at the RPC RS232 Console Port (see Section 4.5.2), a phone line must be connected to the external modem, and the Console Port must be configured for Modem Mode. In addition, your PC must include a communications program.
- **Access via Local PC:** Your PC must be physically connected to the RPC RS232 Console Port as described in Section 4.5.1, the RPC Console Port must be configured for Normal Mode, and your PC must include a communications program.

To access command mode via the Text Interface, proceed as follows:

Note: *When communicating with the unit for the first time, you will not be able to contact the unit via Telnet, until you have accessed command mode, via Local PC or SSH Client, and used the Network Parameters Menu to enable Telnet as described in Section 5.9.*

1. Contact the RPC Unit:

   a) **Via Local PC:** Start your communications program and press **[Enter]**. Wait for the connect message, then proceed to Step 2.

   b) **Via Network:** The RPC includes a default IPv4 format IP address (192.168.168.168) and a default IPv4 format subnet mask (255.255.255.0.) This allows you to contact the unit from any network node on the same subnet, without first assigning an IP Address to the unit. For more information, please refer to Section 5.9.

      i. **Via SSH Client:** Start your SSH client, and enter the RPC IP Address. Invoke the connect command, wait for the connect message, then proceed to Step 2.

      ii. **Via Telnet:** Start your Telnet Client, and then Telnet to the RPC IP Address. Wait for the connect message, then proceed to Step 2.

   c) **Via Modem:** Use your communications program to dial the number for the external modem which you have connected to the RPC Console Port.

2. **Login** / **Password Prompt:** A message will be displayed, which prompts you to enter a username (login name) and password. The default username is "**`super`**" (all lower case, no quotes), and the default password is also "**`super`**".

3. If a valid username and password are entered, the RPC will display the Circuit Status Screen.

   Note: *If a Login Banner has been defined as described in Section 5.3, then a banner page will appear before the command prompt is displayed. The Login Banner can be used to display legal warnings or other information.*

5.1.2. The Web Browser Interface

The Web Browser Interface consists of a series of web forms, which can be used to select configuration parameters and perform reboot operations, by clicking on buttons and/or entering text into designated fields.

> **Note:** *In order to use the Web Browser Interface, Web Access must first be enabled via the Text Interface Network Parameters Menu (/N), the RPC must be connected to a TCP/IP network, and your PC must be equipped with a JavaScript enabled web browser.*

1. Start your JavaScript enabled Web Browser, key the RPC IP address (default = 192.168.168.168) into the web browser's address bar, and press **[Enter]**.
2. **Username** / **Password Prompt:** A message box will prompt you to enter your username and password. The default username is "**`super`**" (all lower case, no quotes), and the default password is also "**`super`**".
3. If a valid username and password are entered, the Circuit Control Screen will be displayed.

   > **Note:** *If a Login Banner has been defined as described in Section 5.3, then a banner page will appear before the command prompt is displayed. The Login Banner can be used to display legal warnings or other information.*

5.1.3. Access Via PDA

In addition to the Web Browser Interface and Text Interface, the RPC command mode can also be accessed by PDA devices. Note however, that due to nature of most PDAs, only a limited selection of RPC operating and status display functions are available to users who communicate with the unit via PDA.

When the RPC is operated via a PDA device, only the following functions are available:

- Product Status Screen (Section 8.1)
- Circuit Status Screen (Section 8.3)
- Circuit Group Status Screen (Section 8.4)
- Circuit Control Screen (Section 9.1.1)
- Circuit Group Control Screen (Section 9.1.2)

These screens will allow PDA users to review Circuit Status and Circuit Group Status, invoke switching and reboot commands and display the Site I.D. and firmware version. Note however, that PDA users are not allowed to change or review RPC configuration parameters.

To configure the RPC for access via PDA, first consult your IT department for appropriate settings. Access the RPC command mode via the Text Interface or Web Browser interface as described in this section, then configure the RPC Network Port accordingly, as described in Section 5.9.

In most cases, this configuration will be adequate to allow communication with most PDAs. Note however, that if you wish to use a BlackBerry® to contact the RPC, you must first make certain to configure the BlackBerry to support HTML tables, as described below:

1. Power on the BlackBerry, and then click on the BlackBerry Internet Browser Icon.
2. Press the Menu button, and then choose "Options."
3. From the Options menu, choose "Browser Configuration," then verify to make certain that "Support HTML Tables" is checked (enabled.)
4. Press the Menu button, and select "Save Options."

When you have finished communicating with the RPC via PDA, it is important to always close the session using the PDA's menu functions, rather than by simply closing the browser window, in order to ensure that the RPC has completely exited from command mode, and is not waiting for the inactivity timeout period to elapse. For example, to close a session on a BlackBerry, press the Menu button and then choose "Close."

5.2. Configuration Menus

Although the Web Browser Interface and Text Interface provide two separate means for selecting parameters, both interfaces allow access to the same set of basic parameters, and parameters selected via one interface will also be applied to the other. To access the configuration menus, proceed as follows:

- **Text Interface:** Refer to the Help Screen (/H) and then enter the appropriate command to access the desired menu. When the configuration menu appears, key in the number for the parameter you wish to define, and follow the instructions in the resulting submenu.
- **Web Browser Interface:** Use the links and fly-out menus on the left hand of the screen to access the desired configuration menu. To change parameters, click in the desired field and key in the new value or select a value from the pull-down menu. To apply newly selected parameters, click on the "Change Parameters" button at the bottom of the menu or the "Set" button next to the field.

The following sections describe options and parameters that can be accessed via each of the configuration menus. Please note that essentially the same set of parameters and options are available to both the Web Browser Interface and Text Interface.

Notes:

- *Configuration menus are only available when you have logged into command mode using a password that permits Administrator Level commands. SuperUser accounts are able to view configuration menus, but are not allowed to change parameters.*
- *Configuration menus are not available when you are communicating with the RPC via PDA*
- *When defining parameters via the Text Interface, make certain to press the **[Esc]** key to completely exit from the configuration menu and save newly defined parameters. When parameters are defined via the Text Interface, newly defined parameters will not be saved until the "Saving Configuration" message has been displayed and the cursor returns to the command prompt.*

5.3. Defining System Parameters

The System Parameters menus are used to define the Site ID Message, set the system clock and calendar, and configure the Invalid Access Lockout feature and Callback feature.

To access the System Parameters menu via the Text Interface, type **/F** and press **[Enter]**. To access the System Parameters menu via the Web Browser Interface, place the cursor over the "General Parameters" link, wait for the flyout menu to appear and then click on the "System Parameters" link. The System Parameters Menus are used to define the following:

- **User Directory:** This function is used to view, add, modify and delete user accounts and passwords. As discussed in Section 5.4 and Section 5.5, the User Directory allows you to set the security level for each account as well as determine which circuits each account will be allowed to control.

  Note: *The "User Directory" option does not appear in the Web Browser Interface's System Parameters menu, and is instead, accessed via the "User Configuration" link on the left hand side of the menu.*

- **Site ID:** A text field, generally used to note the installation site or name for the RPC unit. (Up to 64 characters; Default = undefined)

  Notes:

  - *The Site I.D. will be cleared if the RPC is reset to default settings.*
  - *When viewed via the Text Interface (CLI) Site I.D. messages that are over 30 characters long will be truncated. To display the entire Site I.D. message via the Text Interface, type* ***/J**** *and press* ***[Enter]***

- **Real Time Clock:** This prompt provides access to the Real Time Clock menu, which is used to set the clock and calendar, and to enable and configure the NTP (Network Time Protocol) feature as described in Section 5.3.1.

  Note: *The "Real Time Clock" option does not appear in the Web Browser Interface's System Parameters menu, and is instead, accessed via the "Real Time Clock" link in the General Parameters fly-out menu.*

- **Invalid Access Lockout:** If desired, this feature can be used to temporarily disable Console Port access, SSH access, Telnet access and/or Web access to the RPC command mode after a user specified number of unsuccessful login attempts are made. For more information, please refer to Section 5.3.2.
  (Default = Off)

  Note: *The "Invalid Access Lockout" item does not appear in the Web Browser Interface's System Parameters menu, and is instead, accessed via the link in the General Parameters fly-out menu.*

- **Temperature Format:** Determines whether the temperature is displayed as Fahrenheit or Celsius. (Default = Fahrenheit.)

- **Temperature Calibration:** Used to calibrate the unit's internal temperature sensing abilities. To calibrate the temperature, place a thermometer inside your equipment rack, in a location that usually experiences the highest temperature. After a few minutes, take a reading from the thermometer, and then key the reading into the configuration menu. In the Web Browser Interface, the temperature is entered at the System Parameters menu, in the Temperature Calibration field; in the Text Interface, the temperature is entered in a submenu of the System Parameters menu, accessed via the Temperature Calibration item. (Default = undefined)

- **Log Configuration:** Configures the Audit Log, Alarm Log and Temperature Log. For more information on the RPC's logging functions, please refer to Section 5.3.3. (Defaults: Audit Log = On without Syslog, Alarm Log = On without Syslog, Temperature Log = On)

  Notes:

  - *The Audit Log will create a record of all port connection/disconnection and login/logout activity at the RPC unit.*
  - *The Alarm Log will create a record of each instance where the Invalid Access Alarm is triggered or cleared at the RPC unit.*
  - *The Temperature Log will create a record of ambient rack temperature over time.*

- **Callback Security:** Enables / configures the Callback Security Function as described in Section 5.3.4. In order for this feature to function, a Callback number must also be defined for each desired user account as described in Section 5.5. (Defaults = On - Without Password Prompt, 3 Callback Attempts, 30 Second Callback Delay)

  Notes:

  - *In the Text Interface, Callback Security Parameters are defined via a submenu of the Systems Parameters Menu, which is accessed via the Callback Security item.*
  - *In the Web Browser Interface, Callback Security Parameters are defined via the "Callback Security" link in the General Parameters fly-out menu.*

- **Front Panel Buttons:** This item can be used to disable all Reset button and Default button functions. (Default = On)

- **Modem Phone Number/IP Address:** When an optional external modem is connected to the RPC Console Port, the Modem Phone Number parameter can be used to denote the phone number for the external modem. In cases where the VMR/NPS application includes a cellular modem, the IP address for the cellular modem can be entered via this parameter. (Default = undefined)

- **Management Utility:** Enables/Disables the Enterprise Management Utility (WMU.) When enabled, the WMU allows you to manage multiple WTI units via a single menu. (Default = Off.) For more information on the WMU, please refer to the WMU User's Guide, which can be found on the WTI website at:

  http://www.wti.com/t-product-manuals.aspx

  Note: *Although the Enterprise Management Utility can be enabled/disabled via either the Web Browser Interface and Text Interface, the Management Utility can only be accessed and operated via the Web Browser Interface.*

- **Scripting Options:** Provides access to parameters that are used to set up the VRM/NPS unit for running various scripts as described in Section 5.3.5.

  Note: *In the Text Interface, the Scripting Options submenu is accessed via item 12. To access the Scripting Options parameters via the Web Browser Interface, place the cursor over the "General Parameters" link, wait for the flyout menu to appear, then click on the "Scripting Options" link.*

- **EnergyWise Configuration:** Defines parameters that are needed in order for the RPC to serve as an element in a Cisco® EnergyWise™ network. This item allows the following parameters to be defined. (Default = Off.)

  Note: *In the Web Browser Interface, EnergyWise parameters are defined via the "EnergyWise" link in the General Parameters fly-out menu.*

  - **Enable:** Enables/disables the RPC unit's ability to particapate in a Cisco Energywise network. (Default = Off)
  - **Domain:** The Energywise Domain Name; up to eighty characters long. (Default = undefined.)
  - **Secret:** A password that is used to authenticate each element in a Cisco Energywise network. The Secret parameter can be up to eighty characters long. (Default = undefined.)

- **Asset Tag:** Allows a descriptive tag or tracking number to be assigned to the RPC unit. Once defined, the Asset Tag can be displayed via the Product Status Screen in the Web Interface or via the **`/J*`** command in the Text Interface. (Default = Undefined)

- **Login Banner:** Allows definition of a banner/message that will be displayed when a valid username and password are entered during log in. The Login Banner can be used to post legal warning regarding unauthorized access to the unit or to display other user-defined information or instructions. (Default = Undefined)

  Notes:

  - *Although the Login Banner will be displayed when the RPC is accessed via both the Text Interface and Web Browser Interface, the Login Banner can only be defined via the Text Interface.*
  - *The Login Banner can be up to 1024 characters long.*
  - *The Login Banner text must begin with the* **`<banner>`** *command and end with the* **`</banner>`** *command.*
  - *Banner text can be copied and pasted from a text editor, or sent in from a file.*
  - *For best results, the individual text lines in the Login Banner should be less than 80 characters wide.*

5.3.1. The Real Time Clock and Calendar

The Real Time Clock menu is used to set the RPC internal clock and calendar. The configuration menu for the Real Time Clock offers the following options:

- **Date:** Sets the Month, Day and Year for the RPC real-time clock/calendar.
- **Time:** Sets the Hour, Minute and Second for the RPC real time clock/calendar. Key in the time using the 24-hour (military) format.
- **Time Zone:** Sets the time zone, relative to Greenwich Mean Time. Note that the Time Zone setting will function differently, depending upon whether or not the NTP feature is enabled and properly configured. (Default = GMT (No DST).)
  - **NTP Enabled:** The Time Zone setting is used to adjust the Greenwich Mean Time value (received from the NTP server) in order to determine the precise local time for the selected time zone.
  - **NTP Disabled:** If NTP is disabled, or if the RPC is not able to access the NTP server, then status screens and activity logs will list the selected Time Zone and current Real Time Clock value, but will not apply the correction factor to the displayed Real Time Clock value.
- **NTP Enable:** When enabled, the RPC will contact an NTP server (defined via the NTP Address prompts) once a day, and update its clock based on the NTP server time and selected Time Zone. (Default = Off.)

Notes:

- *The RPC will also contact the NTP server and update the time whenever you change NTP parameters.*
- *To cause RPC to immediately contact the NTP server at any time, make certain that the NTP feature is enabled and configured, then type* **`/F`** *and press* **[Enter]**. *When the System Parameters menu appears, press* **[Esc]**. *The RPC will save parameters and then attempt to contact the server, as specified by currently defined NTP parameters.*

- **Primary NTP Address:** Defines the IP address or domain name (up to 64 characters long) for the primary NTP server. (Default = undefined.)

Notes:

- *In order to use domain names for web addresses, DNS Server parameters must first be defined as described in Section 5.9.5.*
- *The Web Browser Interface includes two separate fields that can be used to define both an IPv4 protocol and IPv6 protocol format Primary NTP Address and Secondary NTP Address.*
- *When the Primary NTP Address and Secondary NTP Address are defined via the Text Interface, the RPC will display a prompt that instructs the user to select IPv4 or IPv6 protocol.*
- *The RPC allows parameters for both IPv4 and IPv6 protocols to be defined and saved.*

- **Secondary NTP Address:** Defines the IP address or domain name (up to 64 characters long) for the secondary, fallback NTP Server. (Default = undefined.)
- **NTP Timeout:** The amount of time in seconds, that will elapse between each attempt to contact the NTP server. When the initial attempt is unsuccessful, the RPC will retry the connection four times. If neither the primary nor secondary NTP server responds, the RPC will wait 24 hours before attempting to contact the NTP server again. (Default = 3 Seconds.)
- **Test NTP Servers:** Allows you to ping the IP addresses or domain names defined via the Primary and Secondary NTP Address prompts, or to ping a new address or domain defined via the Test NTP Servers submenu in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Test NTP Servers feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Test NTP Servers option, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping any user defined IP address in order to make certain that the IP address is responding.*

5.3.2. The Invalid Access Lockout Feature

When properly configured and enabled, the Invalid Access Lockout feature can watch all login attempts made via SSH connection, Telnet connection, web browser or the serial Console Port. If the counter for any of these exceeds the user-defined threshold for maximum invalid attempts, then the corresponding port or protocol will be automatically disabled for the length of time specified by the Lockout Duration parameter.

When Invalid Access Attempt monitoring is enabled for the serial Console Port, the RPC will count invalid access attempts at the serial Console Port. If the number of invalid access attempts exceeds the defined Lockout Attempts trigger value, the RPC will lock the serial Console Port for the defined Lockout Duration period. When Invalid Access Attempt monitoring for SSH, Telnet or Web are selected, a lockout will be triggered when the number of invalid access attempts during the defined Lockout Duration period exceeds the defined Hit Count for the protocol. For example, if the SSH Hit Count is set at 10 and the SSH Lockout Duration period is set at 120 seconds, then if over 10 invalid access attempts are detected within 120 seconds, the RPC will then lock out the MAC address that generated the excessive attempts for 120 seconds.

Note that when an Invalid Access Lockout occurs, you can either wait for the Lockout Duration period to elapse (after which, the RPC will automatically reactivate the port or protocol), or you can issue the /UL command (type **`/UL`** and press **[Enter]**) via the Text Interface to instantly unlock all RPC logical network ports and communication protocols.

Notes:

- *When the Serial Port Invalid Access Lockout Alarm has been enabled as described in Section 7.5, the RPC can also provide notification via email, Syslog Message, and/or SNMP trap whenever an Invalid Access Lockout occurs at the serial Console Port.*
- *If the Network Port has been locked by the Invalid Access Lockout feature, it will still respond to the ping command (providing that the ping command has not been disabled at the Network Port.)*

The Invalid Access Lockout configuration menus allow you to select the following parameters:

- **Serial Port Protection:** Enables/Disables the Invalid Access Lockout function for the serial Console Port and selects lockout parameters. When this item is enabled and excessive Invalid Access attempts are detected at the Console Port, the Console Port will be locked until the user-defined Lockout Duration period elapses, or until the /UL command is issued.
  - **Serial Port Protection:** Enables/Disables the Invalid Access Lockout feature for the serial Console Port. (Default = Off)
  - **Lockout Attempts:** The number of invalid attempts that must occur in order to trigger the Invalid Access Lockout feature at the serial Console Port. (Default = 9)
  - **Lockout Duration:** This option selects the length of time that the serial Console Port will remain locked when Invalid Access Lockout occurs. If the duration is set at "Infinite", then ports will remained locked until the /UL command is issued. (Default = 30 Minutes)

- **SSH Protection:** Enables/Disables and configures the Invalid Access function for SSH connections. When this item is enabled and excessive Invalid Access Attempts via SSH are detected, then the RPC will lock out the offending MAC address for the user-defined SSH Lockout Duration Period or until the /UL command is issued. Note that for SSH protection, the lockout trigger is a function of the SSH Hit Count parameter and the SSH Lockout Duration Parameter.
  - **Lockout Enable:** Enables/Disables Invalid Access Lockout protection for SSH connections. (Default = Off)
  - **SSH Hit Count:** The number of invalid attempts that must occur during the length of time specified by the SSH Lockout Duration period in order to trigger the Invalid Access Lockout feature for SSH protocol. For example, if the SSH Hit Count parameter is set to 10 and the SSH Lockout Duration parameter is set to 30 minutes, then the RPC will lock out the offending MAC address for 30 minutes when over 10 invalid access attempts occur during any 30 minute long period. (Default = 20)
  - **SSH Lockout Duration:** This option selects both the length of time that an SSH Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When an SSH Lockout occurs, the offending MAC address will be prevented from establishing an SSH connection to the RPC for the defined SSH Lockout Duration period. (Default = 2 Seconds)
- **Telnet Protection:** Enables/Disables and configures the Invalid Access function for Telnet connections. When this item is enabled and excessive Invalid Access Attempts via Telnet are detected, then the RPC will lock out the offending MAC address for the user-defined Telnet Lockout Duration Period or until the /UL command is issued. Note that for Telnet protection, the lockout trigger is a function of the Telnet Hit Count parameter and the Telnet Lockout Duration Parameter.
  - **Lockout Enable:** Enables/Disables Invalid Access Lockout protection for Telnet connections. (Default = Off)
  - **Telnet Hit Count:** The number of invalid attempts that must occur during the length of time specified by the Telnet Lockout Duration period in order to trigger the Invalid Access Lockout feature for the Telnet protocol. For example, if the Telnet Hit Count parameter is set to 10 and the Telnet Lockout Duration parameter is set to 30 minutes, then the RPC will lock out the offending MAC address for 30 minutes when over 10 invalid access attempts occur during any 30 minute long period. (Default = 20)
  - **Telnet Lockout Duration:** This option selects both the length of time that a Telnet Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When a Telnet Lockout occurs, the offending MAC address will be prevented from establishing a Telnet connection to the RPC for the defined Telnet Lockout Duration period. (Default = 2 Seconds)

- **Web Protection:** Enables/Disables and configures the Invalid Access function for Web connections. When this item is enabled and excessive Invalid Access Attempts via Web are detected, then the RPC will lock out the offending MAC address for the user-defined Web Lockout Duration Period or until the /UL command is issued. Note that for Web protection, the lockout trigger is a function of the Web Hit Count parameter and the Web Lockout Duration Parameter.
  - **Lockout Enable:** Enables/Disables Invalid Access Lockout protection for web connections. (Default = Off)
  - **Web Hit Count:** The number of invalid attempts that must occur during the length of time specified by the Web Lockout Duration period in order to trigger the Invalid Access Lockout feature for Web access. For example, if the Web Hit Count parameter is set to 10 and the Web Lockout Duration parameter is set to 30 minutes, then the RPC will lock out the offending MAC address for 30 minutes when over 10 invalid access attempts occur during any 30 minute long period. (Default = 20)
  - **Web Lockout Duration:** This option selects both the length of time that a Web Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When a Web Lockout occurs, the offending MAC address will be prevented from establishing a Web connection to the RPC for the defined Telnet Lockout Duration period. (Default = 60 Seconds)

5.3.3. Log Configuration

This feature allows you to create records of command activity, alarm actions and temperature readings for the RPC unit. The Log features are enabled and configured via the System Parameters Menus.

- **Audit Log:** Creates a record of all power switching at the RPC unit, including reboots and switching caused by Load Shedding, Load Shedding Recovery, Ping No Answer Reboots and Scheduled Reboots. Each Log record includes a description of the activity that caused the power switching, the username for the account that initiated the power switching or reboot and the time and date that the power switching or reboot occurred. In addition to power switching activity, the Audit Log will also include login/logout activity for each user account.
- **Alarm Log:** Creates a record of all Alarm Activity at the RPC unit. When an alarm is triggered, the RPC will generate a record that lists the time and date of the alarm, the name of the Alarm triggered, and a description of the Alarm.
- **Temperature Log:** The Temperature Log provides a record of temperature levels over time at the RPC unit. Each Log record will include the time and date, and the temperature reading.

5.3.3.1. Audit Log and Alarm Log Configuration Options

The Log Configuration options in the System Parameters menu allows you to enable/disable and configure the Audit Log and Alarm Log. The Audit Log and Alarm Log both offer the following parameters:

- **Off:** The Log is disabled, and command activity and/or alarm events will not be logged.
- **On - With Syslog:** The Log is enabled, and power switching, login/logout activity and/or alarm events will be logged. The RPC will generate a Syslog Message every time a Log record is created.
- **On - Without Syslog:** The Log is enabled, and power switching, login/logout activity and/or alarm events will be logged, but the RPC will *not* generate a Syslog Message every time a Log record is created. (Default Setting.)

Notes:

- *In order for the Audit Log or Alarm Log to generate Syslog Messages, Syslog Parameters must first be defined as described in Section 11.*
- *The Audit Log will truncate usernames that are longer than 22 characters, and display two dots (..) in place of the remaining characters.*

5.3.3.2. Reading, Downloading and Erasing Logs

To read or download the status logs, proceed as follows:

- **Text Interface:** Type `/L` and press **[Enter]** to access the Display Log menu. Select the desired option, key in the appropriate number, press **[Enter]** and then follow the instructions in the "Display Logs" submenu. In the text interface, The Display Logs menu is used to download or display the Audit Log and Alarm Log.
- **Web Browser Interface:** Move the cursor over the "Logs" link. When the flyout menu appears, click on the desired option and then follow the instructions in the resulting submenu.

Proceed as follows to download, display or erase logged data:

- **Audit Log and Alarm Log:** The Audit Log and Alarm Log can be displayed or downloaded via either the Text Interface or Web Browser Interface. When the Audit Log or Alarm Log are displayed via the Text Interface, the RPC will also offer the option to erase Audit Log or Alarm Log data.
- **Temperature Log:** The Temperature Log can be displayed or downloaded via either the Text Interface or Web Browser Interface. When the Temperature Log is selected via the Text Interface, the RPC will also offer the option to erase Temperature Log data.

5.3.4. Callback Security

The Callback function provides an additional layer of security when callers attempt to access command mode via modem. When this function is properly configured, modem users will not be granted immediate access to command mode upon entering a valid password; instead, the unit will disconnect, and dial a user-defined number before allowing access via that number. If desired, users may also be required to re-enter the password *after* the RPC dials back.

In order for Callback Security to function properly, you must first enable and configure the feature via the System Parameters menu as described in this section, and then define a callback number for each desired user account as described in Section 5.5. To access the Callback Security menu via the Text Interface, type **`/F`** and press **[Enter]** and then select the Callback Security option. To access the Callback Security menu via the Web Browser Interface, place the cursor over the General Parameters link, wait for the flyout menu to appear, and then Click on the "Callback Security" link.

In both the Text Interface and Web Browser Interface, the Callback Security Menu offers the following options:

- **Callback Enable:** This prompt offers five different configuration options for the Callback Security feature: (Default = On - Callback (Without Password Prompt.)
  - **Off:** All Callback Security is disabled.
  - **On - Callback (Without Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the login prompt will *not* be displayed when the user's modem answers. If the account *does not* include a Callback Number, that user will be granted immediate access.
  - **On - Callback (With Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the login prompt *will* be displayed when the user's modem answers (accounts that include a Callback Number will be required to re-enter their username/password when their modem answers.) If the account *does not* include a Callback Number, then that user will be granted immediate access.
  - **On - Callback ONLY (Without Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the username/password prompt will *not* be displayed when the user's modem answers. Accounts that *do not* include a Callback Number will *not* be able to access command mode via modem.
  - **On - Callback ONLY (With Password Prompt):** Callbacks will be performed for accounts that include a Callback Number, and the username/password prompt *will* be displayed when the user's modem answers (users will be required to re-enter their username/password when their modem answers.) Accounts that *do not* include a Callback Number will *not* be able to access command mode via modem.

- **Callback Attempts:** The number of times that the RPC will attempt to contact the Callback number. (Default = 3 attempts.)
- **Callback Delay:** The amount of time that the RPC will wait between Callback attempts. (Default = 30 seconds.)

Notes:

- *After configuring and enabling Callback Security, you must then define a callback phone number for each desired user account (as described in Section 5.5) in order for this feature to function properly.*
- *When using the "On - Callback (With Password Prompt)" option, it is important to remember that accounts that do not include a callback number will be allowed to access command mode without callback verification.*

5.3.5. Scripting Options

The Scripting Options submenu provides access to parameters that are used to set up the RPC unit for running various scripts.

Notes:

- *To access Scripting Options parameters via the Text Interface, first type* **`/F`** *and press* **[Enter]** *to display the System Parameters Menu, then key in the number for the Scripting Options item and press [Enter].*
- *To access the Scripting Options parameters via the Web Browser Interface, place the cursor over the "General Parameters" link, wait for the flyout menu to appear, then click on the "Scripting Options" link.*

The Scripting Options menu allows the following parameters to be defined:

- **Command Confirmation:** Enables/Disables the Command Confirmation feature. When enabled, a "Sure" prompt will be displayed before power switching and reboot commands are executed. When disabled, commands will be executed without further prompting. (Default = On.)
- **Automated Mode:** When enabled, the RPC will execute switching and reboot commands without displaying a confirmation prompt, status screen or confirmation messages. For more information, please refer to Section 5.3.5.1 or Section 9.3. (Default = Off.)

  Note: *When the Automated Mode is enabled, security functions are suppressed, and users are able to access configuration menus and control circuits without entering a password. If security is a concern and the Automated Mode is required, it is recommended to use the IP Security feature (Section 5.9.3) to restrict access.*

- **Command Prompt:** Allows the Text Interface command prompt to be set to either MPC, IPS, NPS, NBB, VMR, CCM, RPC or the current site ID. (Default = RPC.)

- **IPS Mode:** This parameter sets up the RPC for use with command scripts that were written for WTI's IPS Series Remote Reboot Switches. When the IPS Mode is enabled, the "IPS" command prompt will be displayed in the Text Mode, User Accounts will not allow definition of a Username, and only the "password" prompt will be displayed when logging into the unit (IPS Mode units will not display a "username" prompt.) (Default = Off.)
  - The "IPS" command prompt will be displayed in the Text Mode.
  - Providing that no Administrator level user accounts are defined, the RPC will not display the username or password prompts upon login to command mode.
  - If one or more Administrator level user accounts have been defined, then the RPC will only display the password prompt upon login to command mode. If all Administrator level user accounts (aside from the default "super" account) are deleted, then the RPC will return to the status where no username or password prompts are displayed upon login to command mode.
- **Single Plug Boot Delay Enable:** When this parameter is enabled and reboot cycle is initiated, the RPC will pause for the currently defined Boot/Sequence Delay value before executing the next reboot command. Note that the Boot/Sequence Delay value is defined via the Plug Parameters menu, as described in Section 5.7. (Default = On)

5.3.5.1. Automated Mode

The Automated Mode allows the RPC to execute switching and reboot commands, without displaying menus or generating response messages. Automated Mode is designed to allow the RPC to be controlled by a device which can generate commands to control power switching functions without human intervention.

When Automated Mode is enabled, power switching and reboot commands are executed without a confirmation prompt and without command response messages; the only reply to these commands is the command prompt, which is re-displayed when each command is completed.

Although Automated Mode can be enabled using either the Web Browser Interface or Text Interface, Automated Mode is designed primarily for users who wish to send ASCII commands to the RPC without operator intervention, and therefore does not specifically apply to the Web Browser Interface. When Automated Mode is enabled, the Web Browser Interface can still be used to invoke switching and reboot commands.

Notes:

- *When the Automated Mode is enabled, password prompts will not be displayed at login, and you will be able to access Administrator Level command functions (including the configuration menus) and control circuits without entering a password.*
- *If you need to enable the Automated Mode, but want to restrict network access to configuration menus, it is strongly recommended to enable and configure the IP Security Function as described in Section 5.9.3.*

To enable/disable the Automated Mode, go to the System Parameters menu (see Section 5.3,) and then set the “Automated Mode” option to “On”. When Automated Mode is enabled, RPC functions will change as follows:

1. **All Password Security Suppressed:** When a user attempts to access command mode, the password prompt will not be displayed at either the Console Port or Network Port. Unless specifically restricted by the IP Security Function, all users will be allowed to access both switching and configuration functions, and all commands will be immediately accepted without the requirement to enter a password.
2. **Status Screen Suppressed:** The circuit status screen will not be automatically displayed after commands are successfully executed. Note however, that the /S command can still be invoked to display the status screen as needed.
3. **“Sure?” Prompt Suppressed:** All commands are executed without prompting for user confirmation.
4. **Error Messages Suppressed:** Most error messages will be suppressed. Note however, that an error message will still be generated if commands are invoked using invalid formats or arguments.

All other status display and configuration commands will still function as normal.

5.4. User Accounts

Each time you attempt to access command mode, you will be prompted to enter a username and password. The username/password entered at login determine which circuit(s) you will be allowed to control and what type of commands you will be allowed to invoke. Each username/password combination is defined within a "user account."

The RPC allows up to 128 user accounts; each account includes a username, password, security level, circuit access rights, service access rights and an optional callback number.

5.4.1. Command Access Levels

In order to restrict access to important command functions, the RPC allows you to set the command access level for each user account. The RPC offers four access levels: Administrator, SuperUser, User and View Only. Command privileges for each account are set using the "Access Level" parameter in the Add User or Modify User menus.

Each access level grants permission to use a different selection of commands; lower access levels are restricted from invoking configuration commands, while Administrators are granted access to all commands. The four different access levels are listed below:

- **Administrator:** Administrators are allowed to invoke all configuration and power switching commands, can view all status screens, and can always direct switching commands to all RPC switched circuits .
- **SuperUser:** SuperUsers are allowed to invoke all power switching commands and view all status screens. SuperUsers can view configuration menus, but are not allowed to change configuration parameters. SuperUsers are granted access to all RPC circuits.
- **User:** Users are allowed to invoke power switching commands and view all status screens, but can only apply commands to circuits that they are specifically granted access to. In addition, Users are not allowed to view configuration menus or change configuration parameters.
- **ViewOnly:** Accounts with ViewOnly access, are allowed to view Status Menus, but are not allowed to invoke switching commands, and cannot view configuration menus or change parameters. ViewOnly accounts can display the Circuit Status screen, but can only view the status of circuits that are allowed by the account.

Section 17.2 summarizes command access for all four access levels.

In the default state, the RPC includes one predefined account that provides access to Administrator commands and allows control of all RPC switched power circuits. The default username for this account is "**`super`**" (lowercase, no quotation marks), and the password for the account is also "**`super`**".

Notes:

- *In order to ensure security, it is recommended that when initially setting up the unit, a new user account with Administrator access should be created, and the "super" account should then be deleted.*
- *If the RPC is reset to default parameters, all user accounts will be cleared, and the default "super" account will be restored.*

5.4.2. Circuit Access

Each account can be granted access to a different selection of circuits and circuit groups. When accounts are created, the Circuit Access parameter and the Circuit Group Access parameter in the Add User menu or Modify User menu are used to grant or deny access to each circuit or circuit group. In addition, each access level also restricts the circuits and circuit groups that the account will be allowed to access:

- **Administrator:** Administrator level accounts are always allowed to control all circuits and circuit groups. Circuit access cannot be disabled for Administrator level accounts.
- **SuperUser:** SuperUser accounts allow access to all circuits and circuit groups. Circuit access cannot be disabled for SuperUser accounts.
- **User:** User level accounts are only allowed to issue switching commands to the circuits and circuit groups that have been specifically permitted via the "Circuit Access" parameter in the Add User and Modify User menus.
- **ViewOnly:** ViewOnly level accounts are not allowed to issue switching commands. ViewOnly accounts can display the On/Off state of circuits and circuit groups, but are limited to the circuits and circuit groups specified by the account.

5.4.3. Port Access

The Port Access parameter is used to grant or deny access to the RPC DB9 Console Port. Normally, the Console port is used for connection to a local control device or an external modem.

The command access level will also determine which ports the account will be allowed to access, as summarized below:

- **Administrator and SuperUser:** Accounts with Administrator or SuperUser level command access are always allowed to connect to the Console Port. Port access cannot be disabled for Administrator and SuperUser level accounts.
- **User:** User level accounts are only allowed to connect to the Console Port when port access has been specifically enabled for the account.
- **ViewOnly:** Accounts with ViewOnly access are not allowed to create connections to the Console Port.

5.5. Managing User Accounts

The User Directory function is employed to create new accounts, display parameters for existing accounts, modify accounts and delete accounts. Up to 128 different user accounts can be created. The "User Directory" function is only available when you have logged into command mode using an account that permits Administrator commands.

In both the Text Interface and the Web Browser Interface, the User Directory menu offers the following functions:

- **View User Directory:** Displays currently defined parameters for any RPC user account as described in Section 5.5.1.
- **Add Username:** Creates new user accounts, and allows you to assign a username, password, command level, circuit access circuit group access, service access and callback number, as described in Section 5.5.2.
- **Modify User Directory:** This option is used to edit or change account information, as described in Section 5.5.3.
- **Delete User:** Clears user accounts, as described in Section 5.5.4.

Note: *After you have finished selecting or editing user account parameters, make certain to save the new account information before proceeding. In the Web Browser Interface, click on the "Add User" button to save parameters; in the Text Interface, press the* ***[Esc]*** *key several times until the RPC displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.5.1. Viewing User Accounts

The "View User Directory" option allows you to view details about each account. The View User option will not display actual passwords, and instead, the password field will read "defined". The View User Accounts function is only available when you have accessed command mode using a password that permits Administrator Level commands.

5.5.2. Adding User Accounts

The "Add Username" option allows you to create new accounts. Note that the Add User function is only available when you have accessed command mode using a password that permits Administrator Level commands. The Add User Menu can define the following parameters for each new account:

- **Username:** Up to 32 characters long, and cannot include non-printable characters. Duplicate usernames are not allowed. (Default = undefined.)
- **Password:** Five to sixteen characters long, and cannot include non-printable characters. Note that passwords are case sensitive. (Default = undefined.)
- **Access Level:** Determines which commands this account will be allowed to access. This option can set the access level for this account to "Administrator", "SuperUser", "User" or "ViewOnly." For more information on Command Access Levels, please refer to Section 5.4.1 and Section 17.2. (Default = User.)

- **Port Access:** Determines whether or not the account will be allowed to connect to the serial Console Port. (Defaults; Administrator and SuperUser = Always Enabled, User = Disabled.)

  Note: *ViewOnly level accounts cannot be granted access to the Console Port.*

- **Circuit Access:** Determines which circuit(s) this account will be allowed to control. (Defaults; Administrator and SuperUser = All Circuits On, User = All Circuits Off, ViewOnly = All Circuits Off.)

  Notes:

  - *Administrator and SuperUser level accounts always have access to all circuits.*
  - *User level accounts will only have access to the circuits that are defined via the "Circuit Access" parameter.*
  - *ViewOnly accounts are allowed to display the Circuit Status Screen, but are limited to the circuits specified by the account. ViewOnly accounts are not allowed to invoke switching and reboot commands.*

- **Circuit Group Access:** Determines which circuit groups this account will be allowed to control. For more information on Circuit Groups, please refer to Section 5.6. (Defaults; Administrator and SuperUser = All Circuit Groups On, User = All Circuit Groups Off, ViewOnly = All Circuit Groups Off.)

  Notes:

  - *In order to use this feature, Circuit Groups must first be defined as described in Section 5.6.*
  - *Administrator and SuperUser level accounts will always have access to all circuit groups.*
  - *User Level accounts will only have access to the circuit groups that are defined via the Circuit Group Access parameter.*
  - *ViewOnly accounts are allowed to display the On/Off status of circuit groups via the Circuit Status Screen, but are limited to the circuit groups specified by the account. ViewOnly accounts are not allowed to invoke switching and reboot commands.*

- **Service Access:** Determines whether this account will be able to access command mode via Serial Port, Telnet/SSH or Web. For example, if Telnet/SSH Access is disabled for this account, then this account will not be able to access command mode via Telnet or SSH. (Default = Serial Port = On, Telnet/SSH = On, Web = On.)

- **Callback Phone Number:** Assigns a number that will be called when this account attempts to access command mode via modem, and the Callback Security Function has been enabled as described in Section 5.3.4. (Default = undefined.)

Notes:

- *If the Callback Number is not defined, then Callbacks will not be performed for this user.*
- *If the Callback Number is not defined for a given user, and the Callback Security feature is configured to use either of the "On - Callback" options, then this user will be granted immediate access to command mode via modem.*
- *If the Callback Number is not defined for a given user, and the Callback Security feature is configured to use the "On - Callback ONLY" option, then this user will not be able to access command mode via Modem.*
- *When using the "On - Callback (With Password Prompt)" option, it is important to remember that accounts that do not include a callback number will be allowed to access command mode without callback verification.*

Note: *After you have finished selecting or editing account parameters, make certain to save the new account information before proceeding. In the Web Browser Interface, click on the "Add User" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RPC displays the "Saving Configuration" message and the cursor returns to the command prompt.*

- **Authorization Keys:** This item can be used to assign an SSH Authorization Key to the user account, view assigned authorization keys or delete assigned authorization keys. When a valid authorization key is assigned to a given user, that user will be able to access RPC command mode without entering a password. When assigning an authorization key, the RPC offers the option to define a name for the key and upload a key from the user's server.

5.5.3. Modifying User Accounts

The "Edit User Directory" function allows you to edit existing accounts in order to change parameters, circuit access rights or Administrator Command capability. Note that the Edit/Modify User function is only available when you have accessed command mode using a password that permits Administrator Level commands.

Once you have accessed the Modify Users menu, use the menu options to redefine parameters in the same manner employed for the Add User menu, as discussed in Section 5.5.2.

> **Note:** *After you have finished changing parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Modify User" button to save parameters; in the Text Interface, press the* ***[Esc]*** *key several times until the RPC displays the "Saving Configuration" message.*

5.5.4. Deleting User Accounts

This function is used to delete individual user accounts. Note that the Delete User function is only available when you have accessed command mode using a password that permits Administrator Level commands.

Notes:

- *Deleted accounts cannot be automatically restored.*
- *The RPC allows you to delete the default "super" account, which is included to permit initial access to command mode. Before deleting the "super" account, make certain to create another account that permits Administrator Access. If you do not retain at least one account with Administrator Access, you will not be able to invoke Administrator level commands.*

5.6. The Circuit Group Directory

The Circuit Group Directory allows you to designate "groups" of circuits that are dedicated to a similar function, and will most likely be switched or rebooted all at the same time or controlled by the same type of user account.

For example, an individual equipment rack might include an assortment of devices that belong to different departments or clients. In order to simplify the process of granting circuit access rights to the accounts that will control power to these devices, you could assign all of the circuits for the devices belonging to Department A to a Circuit Group named "Dept_A", and all of the circuits for devices belonging to Department B to a Circuit Group named "Dept_B". When user accounts are defined later, this would allow you to quickly grant access rights for all of the circuits for the devices belonging to Department A to the appropriate user accounts, by merely granting access to the Dept_A Circuit Group, rather than by selecting the specific, individual circuits for each user account.

Likewise, Circuit Groups allow you to direct On/Off/Boot commands to a series of circuits, without addressing each circuit individually. Given the example above, you could quickly reboot all circuits for Department A, by either including the "Dept_A" Circuit Group name in a /BOOT command line via the Text Interface, or by using the Circuit Group Control menu in the Web Browser Interface.

The Circuit Group Directory function is only available when you have logged into command mode using an account that permits Administrator commands. In both the Text Interface and the Web Browser Interface, the Circuit Group Directory menu offers the following functions:

- **View Circuit Group Directory:** Displays currently defined circuit access rights for any RPC Circuit Group as described in Section 5.6.1.
- **Add Circuit Group to Directory:** Creates new Circuit Groups, and allows you to assign circuit access rights to each group as described in Section 5.6.2.
- **Modify Circuit Group Directory:** This option is used to edit or change circuit access rights for each Circuit Group, as described in Section 5.6.3.
- **Delete Circuit Group from Directory:** Clears Circuit Groups that are no longer needed, as described in Section 5.6.4.

5.6.1. Viewing Circuit Groups

The "View Circuit Group Directory" option allows you to view the configuration of each Circuit Group. Note that the View Circuit Group Directory function is only available when you have accessed command mode using a password that permits Administrator Level commands. In the Web Browser Interface, the Circuit Group Directory can be viewed by clicking on the link on the left hand side of the page. In the Text Interface, the Circuit Group Directory can be viewed by typing `/G` and pressing **[Enter]** and then selecting the option from the resulting submenu.

5.6.2. Adding Circuit Groups

The "Add Circuit Group to Directory" option allows you to create new Circuit Groups and assign circuit access rights to each group. The Add Circuit Group function is only available when you have accessed command mode using a password that permits Administrator Level commands.

The Add Circuit Group Menu can be used to define the following parameters for each new account:

- **Circuit Group Name:** Assigns a name to the Circuit Group. (Default = undefined)
- **Circuit Access:** Determines which circuits this Circuit Group will be allowed to control. (Default = undefined)

Note: *After you have finished defining or editing Circuit Group parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add Circuit Group" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RPC displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.6.3. Modifying Circuit Groups

The "Modify Circuit Group" function allows you to edit existing Circuit Groups in order to change circuit access rights. Note that this function is only available when you have accessed command mode using a password that permits Administrator Level commands.

Once you have accessed the Modify Circuit Group menu, use the menu options to redefine parameters in the same manner that is used for the Add Circuit Group menu, as discussed in Section 5.6.2.

Note: *After you have finished changing or editing parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Modify Circuit Groups" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RPC displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.6.4. Deleting Circuit Groups

This function is used to delete individual Circuit Groups. Note that this function is only available when you have accessed command mode using a password that permits Administrator Level commands.

Note: *Deleted Circuit Groups cannot be automatically restored.*

5.7. Defining Circuit Parameters

The Circuit Parameters Menu is used to define Circuit Names, boot/sequence delay times and Power Up Default values for each RPC switched circuit. Note that this function is only available when you have accessed command mode using a password that permits Administrator Level commands. The Circuit Parameters Menu allows you to define the following parameters:

- **Circuit Name:** (Up to 24 Characters, Default = undefined.)

  Note: *Circuit Names must begin with either a lower case alphabetic letter or upper case alphabetic letter. Circuit Names cannot begin with a number character or symbol character.*

- **Boot/Seq. Delay:** When more than one circuit is switched On or a reboot cycle is initiated, the Boot/Sequence delay determines how much time will elapse before the next circuit is switched On. When the Boot/Sequence Delay is applied, the RPC will wait for the user-defined delay period before switching On the next circuit. When Reboot cycles and switching actions are initiated, the Boot/Sequence Delay will be applied as follows: (Default = 0.5 Second.)

  - **Reboot Cycle Delay:** During a reboot cycle, the RPC will first switch all selected circuits "Off" (with a 0.5 second pause between each "Off" operation), and then begin to switch selected circuits back On again, pausing for the user-defined Boot/Sequence Delay before switching On the next circuit. For example, if the Boot/Sequence Delay for Circuit 3 is ten seconds, then the RPC will pause for ten seconds before proceeding to the next circuit.

  - **"On" Sequence Delay:** When two or more circuits are switched On, the RPC will pause for the user-defined Boot/Sequence Delay before switching the next circuit.

- **Power Up Default:** Determines how this circuit will react when the Default command (/DPL) is invoked, or after power to the unit has been interrupted and then restored. After the default command is invoked, or power is restored, the RPC will automatically switch each circuit On or Off as specified by the Power-Up Default. (Default = On).

  Note:

  - *If you have accessed command mode using an account that permits Administrator or SuperUser level commands, then the Default command will be applied to all switched circuits.*
  - *If you have accessed command mode via an User Level account, then the Default command will only be applied to circuits allowed by your account.*
  - *The Default command is not available to ViewOnly level accounts.*

- **Boot Priority:** When commands are applied to two or more circuits, the Boot Priority parameter determines the order in which the circuits will be switched On. The circuit that has been assigned a Boot Priority of "1" will always be switched on first, followed by the circuit that has been assigned the Boot Priority of "2", and so forth. When you assign a boot priority to any given circuit, then all subsequent circuits will have their priority lowered by one. For more information on the Boot Priority parameter, please refer to Section 5.7.1. (Default = All circuit prioritized according to Circuit Number)

5.7.1. The Boot Priority Parameter

Normally, when an "On" or "Reboot" command is invoked, the RPC will switch on its circuits in their default, numeric order. Although in many cases, the default, numeric order will work fine, there are other cases where an individual device (such as a router) must be switched on first, in order to support a second device that will be switched on later.

The Boot Priority Parameter simplifies the process of setting the order in which circuits are switched On, by assigning a priority number to each circuit, rather than by requiring the user to make certain that devices are always connected to the RPC in a set order. Likewise, when new devices are added to your equipment rack, the Boot Priority Parameter eliminates the need to disconnect all existing devices and then rearrange the circuits connected to the RPC (and re-define circuit parameters) to ensure that they are switched on in the desired order.

Notes:

- *No two circuits can be assigned the same Boot Priority number.*
- *When a higher Boot Priority is assigned to any given circuit, all subsequent circuits will have their boot priorities lowered by a factor of 1.*
- *The Boot Priority is also displayed on the Circuit Status Screen.*

5.7.1.1. Example 1: Change Circuit A3 to Priority 1

In the Example shown in Figure 5.1, we start out with all Circuits set to their default Boot Priorities, with Circuit A1 first, Circuit A2 second and so forth.

Next, the Boot Priority for Circuit A3 is changed to Priority 1. This means that Circuit A3 will now be switched On first after a reboot, and that Circuit A1 will now be switched On second, Circuit A2 will be third, etc..

Note that when the Boot Priority for Circuit A3 is set to 1, the Boot Priorities for all circuits that were previously Booted before circuit A1 are now lowered by a factor of one.

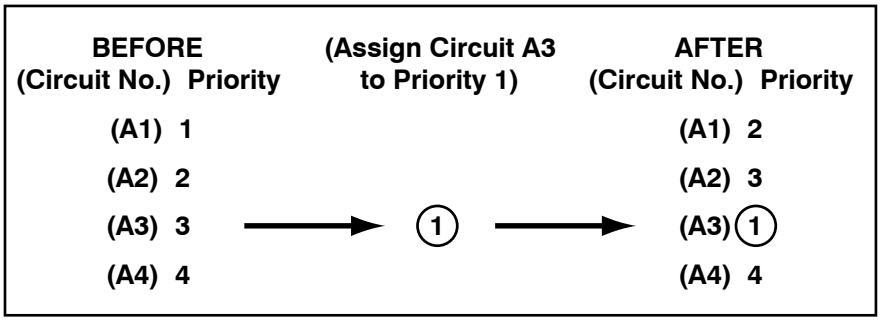

Figure 5.1: Boot Priority Example 1

5.7.1.2. Example 2: Change Circuit A4 to Priority 2

In the second Example shown in Figure 5.2, we start out with Boot Priorities for the circuits set as they were at the end of Example 1; Circuit A3 is first, Circuit A1 is second, Circuit A2 is third and Circuit A4 is fourth.

Next, the Boot Priority for Circuit A4 is changed to Priority 2. This means that Circuit A3 will continue to be switched on first after a reboot, but now Circuit A4 will be switched on second, Circuit A3 will be third and Circuit A2 will be fourth.

Once again, note that when the Boot Priority for Circuit A4 is set to 2, the Boot Priorities for all circuits that were previously Booted before circuit A4 are now lowered by a factor of one

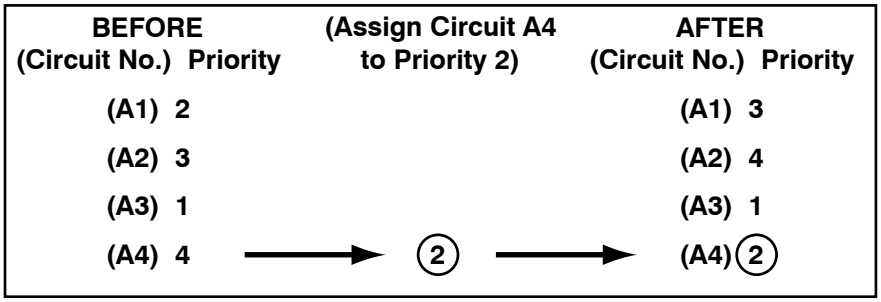

Figure 5.2: Boot Priority Example 2

5.8. Serial Port Configuration

The Port Configuration menu allows you to select parameters for the RPC's serial Console Port. The Console Port (Port 1) can be configured for connection to a local PC or Modem. In addition, the Port Configuration menu (Port Parameters) can also be used to set communications parameters, disable Administrator level commands at the Console Port and also select a number of other parameters described below. The Port Configuration menu allows the following parameters to be defined:

Communication Settings:

- **Baud Rate:** Any standard rate from 300 bps to 115.2K bps. (Default = 9600 bps)
- **Bits/Parity:** (Default = 8-None)
- **Stop Bits:** (Default = 1)
- **Handshake Mode:** XON/XOFF, RTS/CTS (hardware), Both, or None. (Default = RTS/CTS)

General Parameters:

- **Administrator Mode:** In WTI console server products, this parameter is used to permit or deny port access to Administrator level accounts. In RPC products, Administrator access to the serial port cannot be disabled.
- **Logoff Character:** The Logoff Character determines the command(s) or character(s) that must be issued at this port in order to disconnect this port from another port. Note that the Logoff Character does not apply to Direct Connections. (Default = **^x.**)
- **Sequence Disconnect:** Enables/Disables and configures the disconnect command. This item offers the option to disable the Sequence Disconnect, select a one character format or a three character format. (Default = One Character.)
- **Inactivity Timeout:** Enables and selects the Timeout Period for this port. If enabled, the Console Port will disconnect when no additional data activity is detected for the duration of the timeout period. (Default = 5 Minutes.)
- **Command Echo:** Enables or Disables command echo at the Console Port. When disabled, commands that are sent to the Console Port will still be invoked, but the actual keystrokes will not be displayed on your monitor. (Default = On.)
- **Accept Break:** Determines whether the port will accept breaks received from the attached device. When enabled, breaks received at the port will be passed to any port that this port is connected to. When disabled, breaks will be refused at this port. (Default = On.)

Port Mode Parameters:

- **Port Name:** Allows you to assign a name to the Console Port. The Port Name may be up to 24 characters long. (Default = undefined)
- **Port Mode:** The operation mode for this port; Normal Mode, Modem Mode or PPP Modem Mode. (Default = Normal Mode)

  Depending on the Port Mode selected, the RPC will display additional prompts listed below. In the Text Interface, these parameters are accessible via a submenu, which will only be active when the appropriate port mode is selected. In the Web Browser Interface, fields will be "grayed out" unless the corresponding port mode is selected.

  - **Normal Mode:** Allows communication with a local PC and permits access to command mode. When the Normal Mode is selected, the following mode-specific parameter can also be defined:
    - **DTR Output:** Determines how DTR will react when the port disconnects. DTR can be held low, held high, or pulsed for 0.5 seconds and then held high. (Default = Pulse)
  - **Modem Mode:** Permits access to command mode and simplifies connection to an external modem. Modem Mode ports can perform all functions normally available in Normal Mode, but Modem Mode also allows definition of the following, additional parameters:
    - **Modem Reset String:** Redefines the modem reset string. The Reset String can be sent prior to the Initialization string. (Default = **`ATZ`**)
    - **Modem Initialization String:** Defines a command string that can be sent to initialize an external modem to settings required by your application. (Default = **`ATE1M1&C1&D2S0=1&B1&H1&R2`**)
    - **Modem Hang-Up String:** Although the RPC will pulse the DTR line to hang-up an attached modem, the Hang-Up string is often useful for controlling modems that do not use the DTR line. (Default = undefined)
    - **Reset/No Dialtone Interval:** Determines how often the Reset String will be sent to the modem at this port and also sets the trigger value for the No Dialtone Alarm. For more information on the No Dialtone Alarm, please refer to Section 7.8. (Default = 15 Minutes)
    - **No Dialtone Alarm Enable:** When this item is "On" the No Dialtone Alarm can be enabled as described in Section 7.8. When the No Dialtone Alarm is enabled and properly configured, the RPC can provide notification if the unit detects that a phone line connected to a modem installed at this port is dead. (Default = Off)

Note: *When communicating with the RPC via modem, these parameters will not be changed until after you exit command mode and disconnect.*

- **Modem PPP Mode:** Allows data that is normally sent via ethernet to be sent via phone line. When Modem PPP Mode is selected, the following modem-related parameters will be available:
  - **Modem Reset String:** Redefines the modem reset string. The Reset String can be sent prior to the Initialization string. (Default = **`ATZ.`**)
  - **Modem Initialization String:** Defines a command string that is used to initialize the modem to settings required for PPP communication (Default = **`ATQ0V1E1S0=0&C1&D2`**)
  - **Modem Hang-Up String:** Although the RPC will pulse the DTR line to hang-up an attached modem, the Hang-Up string is often useful for controlling modems that do not use the DTR line. (Default = undefined.)
  - **Reset/No Dialtone Interval:** Determines how often the Reset String will be sent to the modem at this port and also sets the trigger value for the No Dialtone Alarm. For more information on the No Dialtone Alarm, please refer to Section 7.8. (Default = 15 Minutes)
  - **No Dialtone Alarm Enable:** When this item is "On" the No Dialtone Alarm can be enabled as described in Section 7.8. When the No Dialtone Alarm is enabled, the RPC can provide notification if the unit detects that a phone line connected to a modem installed at this port is dead. (Default = Off.)
  - **Periodic Reset Location:** The IP address or URL for the website that will be used to keep the PPP connection alive when not in use. The RPC will regularly ping the selected IP address or URL in order to keep the connection alive. (undefined)

Notes:

- *In order to select a domain name as the Periodic Reset Location, you must first define the Domain Name Servers as described in Section 5.9.5.*
- *The IP Address, P-t-P and Subnet Mask parameters cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication is started..*

  - **PPP Phone Number:** The phone number for the line that will be used for PPP communication. (undefined)
  - **User Name:** The user name for the ISP account that will be used for PPP communication. (undefined)
  - **Password:** The password for the ISP count that will be used for PPP communication (undefined)
  - **IP Address:** The temporary IP address that will be assigned to the PPP communication session by the ISP. Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started. (undefined)
  - **P-t-P:** Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started. (undefined)
  - **Subnet Mask:** Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started. (undefined)

5.9. Network Configuration

The Network Parameters Menus are used to select parameters and options for the Network Port and also allow you to implement IP Security features, which can restrict access based on the user's IP Address.

Although the Web Browser Interface and Text Interface allow definition of essentially the same parameters, parameters are arranged differently in the two interfaces. In the Text Interface, most network parameters are defined via one menu which is accessed using the /N command. In the Web Browser Interface, network parameters are divided into separate menus which are accessed via the Network Configuration flyout menu.

Notes:

- *Settings for network parameters depend on the configuration of your network. Please contact your network administrator for appropriate settings.*
- *The Network Parameters Menu selects parameters for all 16 logical Network Ports.*
- *The IP Address, Subnet Address and Gateway Address cannot be changed via the Web Browser Interface. In order to change these parameters, you must access the unit via the Text Interface.*
- *When a new IP Address is selected, or the status of the DHCP feature is changed, the unit will disconnect and reconfigure itself with the new values when you exit the Network Parameters Menu. When configuring the unit, make certain your DHCP server is set up to assign a known, fixed IP address in order to simplify reconnection to the unit after the new address has been assigned. DHCP Parameters cannot be changed via the Web Browser Interface.*
- *The Network Parameters menu is only available when you have logged into command mode using an account and port that permit Administrator level commands (Supervisor Mode enabled.)*

The Network Parameters menu allows you to define the parameters discussed in the following sections. Note that although the descriptions of network parameters are arranged according to the Web Browser Interface, in the Text Interface, most parameters are found in two large menus: one for IPv4 and one for IPv6. Note that both the IPv4 configuration menu and the IPv6 configuration menu offer essentially the same parameters. To access the network configuration menus, proceed as follows

- **Text Interface:** To define network parameters for the IPv4 protocol, type **`/N`** and press **[Enter]**. To define network parameters for the IPv6 protocol, type **`/N6`** and press **[Enter]**.
- **Web Browser Interface:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the appropriate link to display the desired menu. Note that some submenus offer the option to define IPv4 or IPv6 parameters and that IPv4 and IPv6 menus include a button that can be used to jump to the other protocol.

5.9.1. Network Port Parameters

In the Text Interface, these parameters are found in the main Network Configuration menu In the Web Browser Interface, these parameters are found by placing the cursor over the "Network Configuration" link on the left hand side of the screen, and then clicking on the "Network Port Parameters" link in the resulting fly-out menu.

- **Administrator Mode:** Permits/denies port access to accounts that allow Administrator or SuperUser level commands. When enabled (Permit), the port will be allowed to invoke Administrator and SuperUser level commands, providing they are issued by an account that permits them. If disabled (Deny), then accounts that permit Administrator and SuperUser level commands will not be allowed to access command mode via this port. (Default = Permit)

- **Logoff Character:** Defines the Logoff Character for this port. This determines which command(s) must be issued at this port in order to disconnect from a second port. (Default = **^x** (**[Ctrl]** plus **[X]**))

  Note: *The Sequence Disconnect parameter can be used to pick a one character or a three character logoff sequence.*

- **Sequence Disconnect:** Enables/Disables and configures the Resident Disconnect command. Offers the option to either disable the Sequence Disconnect, or select a one character, or three character command format. (Default = One Character).

  Notes:

  - *The One Character Disconnect is intended for situations where the destination port should **not** receive the disconnect command. When the Three Character format is selected, the disconnect sequence **will** pass through to the destination port prior to breaking the connection.*
  - *When Three Character format is selected, the Resident Disconnect uses the format* "**[Enter]**`LLL`**[Enter]**"*, where* `L` *is the selected Logoff Character.*

- **Inactivity Timeout:** Enables and selects the Inactivity Timeout period for the Network Port. If enabled, and the port does not receive or transmit data for the specified time period, the port will disconnect. (Default = 5 Minutes)

- **Command Echo:** Enables or Disables the command echo for the Network Port. (Default = On)

- **Accept Break:** Determines whether the port will accept breaks received from the attached device, and pass them along to a connected port. When enabled, breaks received at this port will be passed to any port this port is connected to, and sent to the device connected to the other port. When disabled, breaks will be refused at this port. (Default = On)

- **Multiple Logins:** (Text Interface Only) If the RPC is installed in an environment that *does not* include communication via an open network (local communication only), then the Multiple Logins parameter can be used to determine whether or not multiple users will be able to communicate with the unit at the same time. If this parameter is set to "Off" then only one user will be allowed to communicate with the unit at a time. (Default = On)

5.9.2. Network Parameters

In the Text Interface, these parameters are accessed via the main Network Configuration menu, which can be activated by typing **/N** (for IPv4 parameters) or **/N6** (for IPv6 parameters) and then pressing **[Enter]**. In the Web Browser Interface, these parameters are found by placing the cursor over the "Network Configuration" link on the left hand side of the screen, and then clicking on the "Network Parameters" link in the resulting fly-out menu.

Note: *The IP Address, Subnet Mask, Gateway Address and DHCP status cannot be changed via the Web Browser Interface. In order to change these parameters, you must access the RPC via the Text Interface.*

- **IP Address:** (Defaults: IPv4 = 192.168.168.168; IPv6= undefined)
- **Subnet Mask:** (IPv4 Only; Default = 255.255.255.0)
- **Subnet Prefix:** (IPv6 Only; Default = undefined)
- **Gateway Address:** (Default = undefined)
- **DHCP:** Enables/Disables Dynamic Host Configuration Protocol. When this option is "On", the RPC will perform a DHCP request. Note that in the Text Interface, the MAC address for the RPC is listed on the Network Status Screen. (Default = Off)

  Note: *Before configuring this feature, make certain your DHCP server is set up to assign a known, fixed IP address. You will need this new IP address in order to reestablish a network connection with the RPC unit.*

- **IP Security:** Provides access to a submenu that is used to enable and define the IP Security filter as described in Section 5.9.3. (Default = Off)
- **Static Route:** Provides access to a submenu that is used to enable and define Static Route functions as described in Section 5.9.4. (Default = Off)
- **DNS Servers:** Provides access to a submenu that is used to define Domain Name Server parameters as described in Section 5.9.5. (Default = undefined)
- **Negotiation:** (Text Interface Only) This parameter can be used to solve synchronization problems when the RPC unit negotiates communication parameters with another device. (Default = Auto)

  Notes:

  - *If the other device is set for automatic negotiation, then the RPC's Negotiation parameter should also be set to Auto.*
  - *If the other device is not set for automatic negotiation, then the RPC's Negotiation parameter should be set to match the other device (e.g., "100/Full.)*

- **Telnet Access:** Enables/disables Telnet access. When Telnet Access is "Off," users will not be allowed to establish a Telnet connection to the unit. Note that in the Text Interface, this item also provides access to the "Telnet Port" and "Maximum per Source" parameters. (Default = Off)
- **Telnet Port:** Selects the TCP/IP port number that will be used for Telnet connections. In the Text Interface, this item is defined via a submenu, displayed when the Telnet Access parameter is selected. (Default = 23)

- **Max. Per Source:** The maximum number of Telnet sessions that will be allowed per user MAC address. (Default = 4)

Notes:

- *In the Text Interface, the "Per Source" parameter is defined via a submenu of item 21 (Telnet Access) in the Network Parameters menu.*
- *After changing the "Max Per Source" parameter, you must log out of all pre-existing Telnet sessions in order for the new maximum value to be applied.*

- **SSH Access:** Enables/disables SSH communication. (Default = On.)
- **SSH Port:** Selects the TCP/IP port number that will be used for SSH connections. Note that in the Text Interface, this option is defined via a submenu that is displayed when the SSH Access parameter is selected (item number 22). (Default = 22.)
- **HTTP Access (Web Access):** Enables/disables the Web Browser Interface. When disabled, users will not be allowed to contact the unit via the Web Browser Interface. (Default = Off.)
- **HTTP Port:** Selects the TCP/IP port number that will be used for Web Access. (Default = 80.)
- **HTTPS Access:** Enables/disables HTTPS communication. For instructions on setting up SSL encryption, please refer to Section 14. (Default = Off.)
- **HTTPS Port:** Selects the TCP/IP port number that will be used for HTTPS connections. (Default = 443.)

Notes:

- *In the Text Interface, HTTP and HTTPS parameters reside in a separate submenu. To enable and configure HTTP and HTTPS Access via the Text Interface, access the Network Configuration Menu as described in Section 5.9, then type* **23***, press* ***[Enter]*** *and use the resulting submenu (Figure 14.1) to select parameters as described in Section 14.*
- *When the Web Access parameter is defined via the Text Interface, the resulting submenu will also allow you to select SSL (encryption) parameters as described in Section 14.*

- **Harden Web Security:** When the Harden Web Security feature is On (default,) only the high and medium cypher suites for SSLv3 and TLSv1 will be enabled. When the Harden Web Security feature is Off, all SSL protocols will be enabled, allowing compatibility with older browsers. Note that in the Text Interface, this option is enabled/disabled via the Web Access submenu. (Default = On.)
- **TLS Mode:** Selects TLSv1 or TLSv1.1. Although TLSv1.1 provides better security, the default settings of most browsers do not support TLSv1.1. For more information, please refer to Section 14.4. (Default = TLSv1)

Note: *In the Text Interface, the TLS Mode parameter is located in the Web Access submenu.*

- **SYSLOG Addresses:** Defines the IP addresses for the Syslog Daemon(s) that will receive log records generated by the RPC. Allows definition of IP addresses for both a primary Syslog Daemon and an optional secondary Syslog Daemon. SYSLOG Addresses can be entered in either IPv4 or IPv6 format, or in domain name format (up to 64 characters.) For more information, please refer to Section 11. (Default = undefined.)

Notes:

- *The RPC includes a Ping Test (Ping Syslog Address) function that is used to ping the user-selected Syslog IP Address to verify that a valid IP address has been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping the currently defined Syslog Addresses in order to make certain that the IP addresses are responding.*

- **Ping Access:** Configures the RPC's response to ping commands. Ping Access can be set to block all ping commands, allow all ping commands or only accept ping commands from user specified IP addresses (Limited.) When the "Limited" option is selected, up to four permitted IP address can be defined via the submenu. Note that disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm. (Default = Allow All)

- **Raw Socket Access:** Enables/disables Raw Socket Protocol access to the Network Port via Direct Connect and selects the port number for Raw Socket Access. This item can be used to enable or disable Raw Socket Protocol access and select either port 23 or port 3001 for use for Raw Socket connections. (Default = Off.)

Notes:

- *The Raw Socket Access option is often useful for users who encounter network problems when attempting to communicate with the RPC using a script that was previously written for our legacy IPS product line.*
- *If the "On (23)" option is selected, you must either disable Telnet Port 23 or use the Telnet Access option to select a port other than Port 23.*
- *When the Raw Socket Access option is enabled, you must connect to the RPC using the port number selected for Raw Socket Access. For example, if the RPC IP address is "1.2.3.4", and port 3001 has been selected for Raw Socket Acess, in order to establish a Raw Socket connection to the RPC's Network Port, then on a UNIX system, the connection command would be:* `$ telnet 1.2.3.4 3001` ***[Enter]***.

- **Ping Syslog Servers:** (Ping Test) Pings the IP addresses which have been defined for the SYSLOG Severs in order to check for a response.

Notes:

- *The Syslog Address submenu in the Text Interface and the Network Parameters submenu in the Web Browser Interface both include a Ping Test function that can be used to ping the user-selected Syslog IP Addresses in order to verify that valid IP addresses have been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping the currently defined Syslog Addresses in order to make certain that the IP addresses are responding.*

5.9.3. IP Security

The IP Security feature allows the RPC to restrict unauthorized IP addresses from establishing inbound connections to the unit via telnet or Web Browser. This allows you to grant access to only a specific group of Telnet or Web IP addresses, or block a particular IP address completely. In the default state, the RPC accepts incoming IP connections from all hosts.

In the Text Interface, IP Security parameters are defined via the Network Configuration menu. In the Web Browser Interface, these parameters are found by placing the cursor over the "Network Configuration" link, and then clicking on the "IP Security" link in the resulting fly-out menu. In the default state, IP Security is disabled. The IP Security Function employs a TCP Wrapper program which allows the use of standard, Linux operators, wild cards and net/mask pairs to create a host based access control list.

The IP Security configuration menus include "hosts.allow" and "hosts.deny" client lists. When setting up IP Security, you must enter IP addresses for hosts that you wish to allow in the Allow list, and addresses for hosts that you wish to deny in the Deny list. Since Linux operators, wild cards and net/mask pairs are allowed, these lists can indicate specific addresses, or a range of addresses to be allowed or denied.

When the IP Security feature is properly enabled, and a client attempts to connect, the RPC will perform the following checks:

1. If the client's IP address is found in the "hosts.allow" list, the client will be granted immediate access. Once an IP address is found in the Allow list, the RPC will not check the Deny list, and will assume you wish to allow that address to connect.
2. If the client's IP address is not found in the Allow list, the RPC will then proceed to check the Deny list.
3. If the client's IP Address *is* found in the Deny list, the client *will not* be allowed to connect.
4. If the client's IP Address *is not* found in the Deny list, the client *will* be allowed to connect, even if the address was not found in the Allow list.

Notes:

- *If the RPC finds an IP Address in the Allow list, it will not check the Deny list, and will allow the client to connect.*
- *If both the Allow and Deny lists are left blank, then the IP Security feature will be disabled, and all IP Addresses will be allowed to connect (providing that the proper password and/or SSH key is supplied.)*
- *When the Allow and Deny lists are defined, the user is only allowed to specify the Client List; the Daemon List and Shell Command cannot be defined.*

5.9.3.1. Adding IP Addresses to the Allow and Deny Lists

To add an IPv4 or IPv6 format IP Address to the Allow or Deny list, and begin configuring the IP Security feature, proceed as follows.

Notes:

- *Both the Allow and Deny list can include Linux operators, wild cards, and net/mask pairs.*
- *In some cases, it is not necessary to enter all four "digits" of the IP Address. For example, if you wish to allow access to all IP addresses that begin with "192," then you would only need to enter "192."*
- *The IP Security Configuration menu is only available when you have accessed command mode using an account that permits Administrator level commands.*
- *In order to use domain names in the Allow List and/or Deny List, you must first define IP address(es) for the desired Domain Name Server(s) as described in Section 5.9.5.*

1. Access the IP Security Configuration Menu.

   a) **Text Interface:** Type **`/N`** **[Enter]** to define addresses in IPv4 format, or type **`/N6`** and press **[Enter]** to define addresses in IPv6 format. The Network Configuration Menu will be displayed. From the Network Configuration Menu, type **`5`** **[Enter]** to display the IP Security Menu.

   b) **Web Browser Interface:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "IP Security" Link to display the IP Security Menu. The IP Security menu in the Web Browser Interface will accept addresses in either IPv4 or IPv6 format.

2. **Allow List:** Enter the IP Address(es) for the clients that you wish to allow. Note that if an IP Address is found in the Allow list, the client will be allowed to connect, and the RPC will not check the Deny list.

   a) **Text Interface:** Note the number for the first empty field in the Allow list, then type that number at the command prompt, press **[Enter]**, and then follow the instructions in the resulting submenu.

   b) **Web Browser Interface:** Place the cursor in the first empty field in the parameters menu, then key in the desired IP Address, operators, wild cards, and/or net/mask pairs.

3. **Deny List:** Enter the IP Address(es) for the clients that you wish to deny. Note that if the client's IP Address is not found in the Deny List, that client will be allowed to connect. Use the same procedure for entering IP Addresses described in Step 2 above.

5.9.3.2. Linux Operators and Wild Cards

In addition to entering a specific IP address or partial IP address in the Allow or Deny list, you may also use standard Linux operators or wild cards. In most cases, the only operator used is "EXCEPT" and the only wild card used is "ALL," but more experienced Linux users may note that other operators and wild cards may also be used.

EXCEPT: This operator creates an exception in either the "allow" list or "deny" list. For example, if the Allow list includes a line which reads "192. EXCEPT 192.255.255.6," then all IP address that begin with "192." will be allowed; except 192.255.255.6 (providing that this address appears in the Deny list.)

ALL: The ALL wild card indicates that all IP Addresses should be allowed or denied. When ALL is included in the Allow list, all IP addresses will be allowed to connect; conversely, if ALL is included in the Deny list, all IP Addresses will be denied (except for IP addresses listed in the Allow list.) For example, if the Deny list includes a line which reads "ALL EXCEPT 168.255.192.192," then all IP addresses except 168.255.192.192 will be denied (except for IP addresses that are listed in the Allow list.)

Net/Mask Pairs: An expression of the form "n.n.n.n/m.m.m.m" is interpreted as a "net/mask" pair. A host address is matched if "net" is equal to the bitwise AND of the address and the "mask." For example, the net/mask pattern "131.155.72.0/255.255.254.0" matches every address in the range "131.155.72.0" through "131.155.73.255."

5.9.3.3. IP Security Examples

1. **Mostly Closed:** Access is denied by default and the only clients allowed, are those explicitly listed in the Allow list. To deny access to all clients except 192.255.255.192 and 168.112.112.05, IP Security would be defined as follows:

   - Allow List:
     1. 192.255.255.192
     2. 168.112.112.05
   - Deny List:
     1. ALL

2. **Mostly Open:** Access is granted by default, and the only clients denied access, are those explicitly listed in the Deny list. To allow access to all clients except 192.255.255.192 and 168.112.112.05, the IP Security would be defined as follows:

   - Allow List:
     1. ALL EXCEPT 192.255.255.192, 168.112.112.05
   - Deny List:
     1. 192.255.255.192, 168.112.112.05

Notes:

- *When defining a line in the Allow or Deny list that includes several IP addresses, each individual address is separated by either a space, a comma, or a comma and a space as shown in Example 2 above.*
- *Take care when using the "ALL" wild card. When ALL is included in the Allow list, it should always include an EXCEPT operator in order to allow the unit to proceed to the Deny list and determine any addresses you wish to deny.*

5.9.4. Static Route

The Static Route menu allows you to type in Linux routing commands that will be automatically executed each time that the unit powers up or reboots. In the Text Interface, the Static Route menu is accessed via the Network Configuration menu. In the Web Browser Interface, the Static Route menu via the Network Configuration flyout menu. Note that parameters defined via this menu will be applied to both IPv4 and IPv6 communication.

5.9.5. Domain Name Server

The DNS menu is used to select IP addresses for Domain Name Servers. When web and network addresses are entered, the Domain Name Server interprets domain names (e.g., www.yourcompanyname123.com), and translates them into IP addresses. Note that if you don't define at least one DNS, then IP addresses must be used, rather than domain names. Note that parameters defined via this menu will be applied to both IPv4 and IPv6 communication.

When accessed via the Text Interface, the Domain Name Server menu includes a Ping Test feature, that allows you to ping the IP addresses for each user-defined domain name server in order to check that a valid IP address has been entered.

Note: *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*

5.9.6. SNMP Access Parameters

These menus are used to select access parameters for the SNMP feature. The SNMP Access Parameters Menu allows the following parameters to be defined:

Notes:

- *After you have configured SNMP Access Parameters, you will then be able to manage the RPC User Directory, control power and reboot switching and display unit status via SNMP, as described in Section 13.*
- *In the Text Interface, SNMP Access Parameters are defined via two separate menus that are accessed via either the* **/N** *command (IPv4) or the* **/N6** *command (IPv6.)*
- *In the Web Browser interface, both IPv4 and IPv6 SNMP Access Parameters are defined via a single menu. When defining IPv6 parameters, make certain that the IPv6 checkbox in the SNMP Access Parameters menu is checked.*

- **Enable:** Enables/disables SNMP Polling. (Default = Off)

  Note: *This item only applies to external SNMP polling of the RPC; it does not effect the ability of the RPC to send SNMP traps.*

- **Version:** Determines which SNMP Version the RPC will respond to. For example, if this item is set to V3, then clients who attempt to contact the RPC using SNMPv2 will not be allowed to connect. (Default = V1/V2 Only)

- **Read Only:** Enables/Disables the "Read Only Mode", which controls the ability to access configuration functions and invoke switching commands. When Enabled ("Yes"), you will not be able to change configuration parameters or invoke other commands when you contact the RPC via SNMP. (Default = No.)

  Note: *In order to define user names for the RPC via your SNMP client, the Read Only feature must be disabled. When the Read Only feature is enabled, you will not be able to issue configuration commands to the RPC unit via SNMP.*

- **Authentication** / **Privacy:** Configures the Authentication and Privacy features for SNMPv3 communication. The Authentication / Privacy parameter offers two options, which function as follows:

  1. **Auth**/**noPriv:** An SNMPv3 username and password will be required at log in, but encryption will not be used. (Default Setting.)
  2. **Auth**/**Priv:** An SNMPv3 username and password will be required at log in, and all messages will be sent using encryption.

  Notes:

  - *The Authentication / Privacy item is not available when the Version parameter is set to V1/V2.*
  - *If the Version Parameter is set to V1/V2/V3 (all) and Authentication / Privacy parameter is set to "Auth/Priv", then only V3 data will be encrypted.*
  - *The RPC supports DES encryption, but does not currently support the AES protocol.*
  - *The RPC does not support "noAuth/noPriv" for SNMPv3 communication.*

- **SNMPv3 User Name:** Sets the User Name for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2. (Default = undefined.)

- **SNMPv3 Password:** Sets the password for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2. (Default = undefined.)

- **SNMPv3 Password Confirm:** This prompt is used to confirm the SNMPv3 password that was entered at the prompt above. Note that this option is not available when the Version parameter is set to V1/V2. (Default = undefined.)

- **Authentication Protocol:** This parameter determines which authentication protocol will be used. The RPC supports both MD5 and SHA1 authentication. (Default = MD5.)

  Notes:

  - *The Authentication Protocol that is selected for the RPC must match the protocol that your SNMP client will use when querying the RPC unit.*
  - *The Authentication Protocol option is not available when the Version parameter is set to V1/V2*

- **Privacy Protocol:** (SNMPv3 Only) Selects AES or DES encryption support. (Default = DES)

- **SNMP Contact:** (Default = undefined.)
- **SNMP Location:** (Default = undefined.)
- **Read Only Community:** Note that this parameter is not available when the SNMP Version is set to V3. (Default = Public.)
- **Read/Write Community:** Note that this parameter is not available when the SNMP Version is set to V3. (Default = Public.)

5.9.7. SNMP Trap Parameters

These menus are used to select parameters that will be employed when SNMP traps are sent. For more information on SNMP Traps, please refer to Section 12. Both the Text Interface and Web Browser Interface allow the following parameters to be defined:

Notes:

- *In the Text Interface, SNMP Trap parameters are defined via two separate menus that are accessed via either the* **/N** *command (IPv4) or the* **/N6** *command (IPv6.)*
- *In the web browser interfrace, SNMP Trap parameters are defined via two separate submenus that are accessed via the IPv4 or IPv6 flyout menus, under the SNMP Traps link.*

- **SNMP Manager 1:** The IP Address for the first SNMP Manager. For more information, please refer to Section 12. (Default = Undefined)

  Note: *In order to enable the SNMP Trap feature, you must define at least one SNMP Manager.*

- **SNMP Manager 2:** (Default = undefined)
- **Trap Community:** (Default = Public)
- **Trap Version:** The assigned security level for SNMP traps. (Default = V1)
- **V3 Trap Engine ID:** The V3 SNMP agent's unique identifier. (Default = undefined)
- **Ping Test:** Allows you to ping the IP addresses or domain names defined via the SNMP Manager 1 and SNMP Manager 2 prompts in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping the currently defined SNMP Managers in order to make certain that the IP addresses are responding.*

5.9.8. LDAP Parameters

The RPC supports LDAP (Lightweight Directory Access Protocol,) which allows authentication via the "Active Directory" network Directory Service. When LDAP is enabled, command access rights can be granted to new users without the need to define individual new accounts at each RPC unit, and existing users can also be removed without the need to delete the account from each RPC unit. This also allows administrators to assign users to LDAP groups, and then specify which plugs the members of each group will be allowed to control at each RPC unit.

In order to apply the LDAP feature, you must first define User Names and associated Passwords and group membership via your LDAP server, and then access the RPC command mode to configure LDAP settings and define port access rights and command access rights for each group specified at the LDAP server. To access the LDAP Parameters menu, login to RPC command mode using a password that permits Administrator level commands. In the Text Interface, the LDAP Parameters menu is accessed via the Network Configuration menu (/N for IPv4 parameters or /N6 for IPv6 parameters.) In the Web Browser Interface, both IPv4 and IPv6 parameters are defined via a single LDAP Parameters menu, which is accessed via the flyout menus under the Network Configuration link.

Notes:

- *In the Text Interface, the LDAP Parameters menu is accessed via the Network Configuration menu (/N for IPv4 parameters or /N6 for IPv6 parameters.)*
- *In the Web Browser Interface, both IPv4 and IPv6 parameters are defined via a single LDAP Parameters menu, which is accessed via the flyout menus under the Network Configuration link.*
- *Circuit access rights are not defined at the LDAP server. They are defined via the LDAP Group configuration menu on each RPC unit and are specific to that RPC unit alone.*
- *When LDAP is enabled and properly configured, LDAP authentication will supersede any passwords and access rights that have been defined via the RPC user directory.*
- *If no LDAP groups are defined on a given RPC unit, then access rights will be determined as specified by the "default" LDAP group.*
- *The "default" LDAP group cannot be deleted.*

The LDAP Parameters Menu allows you to define the following parameters:

- **Enable:** Enables/disables LDAP authentication. (Default = Off)
- **Primary Host IPv4:** Defines the IP address or domain name for the primary LDAP server when IPv4 protocol is used to communicate with the VMR/NPS unit. (Default = undefined)
- **Primary Host IPv6:** Defines the IP address or domain name for the primary LDAP server when IPv6 protocol is used to communicate with the VMR/NPS unit. (Default = undefined)
- **Secondary Host IPv4:** Defines the IP address or domain name for the secondary (fallback) LDAP server when IPv4 protocol is used. (Default = undefined)
- **Secondary Host IPv6:** Defines the IP address or domain name for the secondary (fallback) LDAP server when IPv6 protocol is used. (Default = undefined)

- **LDAP Port:** Defines the port that will be used to communicate with the LDAP server. (Default = 389)
- **TLS/SSL:** Enables/Disables TLS/SSL encryption. Note that when TLS/SSL encryption is enabled, the LDAP Port should be set to 636. (Default = Off)
- **Bind Type:** Sets the LDAP bind request password type. In the Text Interface, when the Bind Type is set to "Kerberos," the LDAP menu will include an additional prompt used to select Kerberos parameters. In the Web Interface, Kerberos parameters are defined using the prompts at the bottom of the menu. (Default = Simple)
- **Search Bind DN:** The username that will be allowed to search the LDAP directory. (Default = undefined)
- **Search Bind Password:** The Password for the user who is allowed to search the LDAP directory. (Default = undefined.)
- **User Search Base DN:** The directory location for user searches. (Default = undefined.)
- **User Search Filter:** Selects the attribute that lists the user name. Note that this attribute should always end with "=%s" (no quotes.) (Default = undefined.)
- **Group Membership Attribute:** Selects the attribute that list group membership(s). (Default = undefined.)
- **Group Membership Value Type:** (Default = DN.)
- **Fallback:** Enables/Disables the LDAP fallback feature. When enabled, the RPC will revert to it's own internal user directory (see Section 5.5) if no defined users are found via the LDAP server. In this case, port access rights will then be granted as specified in the default LDAP group. (Default = Off.)
- **LDAP Kerberos Set Up:** Kerberos is a network authentication protocol, which provides a secure means of identity verification for users who are communicating via a non-secure network. In the Text Interface, Kerberos parameters are selected via a submenu that is only available when Kerberos is selected as Bind Type. In the Web Browser Interface, Kerberos parameters are defined via the main LDAP Parameters menu. The following parameters are available:.
  - **Port:** (Default = 88.)
  - **Realm:** (Default = Undefined.)
  - **Key Distribution Centers (KDC1 through KDC5):** (Default = Undefined.)
  - **Domain Realms 1 through 5:** (Default = Undefined.)
- **LDAP Group Set Up:** Provides access to a submenu, which is used to define LDAP Groups as described in the Sections 5.9.8.1 through 5.9.8.4.

- **Debug:** This option is used to assist WTI Technical Support personnel with the diagnosis of LDAP issues. (Default = Off.)
- **Ping Test:** (Text Interface Only) Allows you to ping IP addresses or domain names that have been defined via the LDAP Parameters menus in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping any user defined IP address in order to make certain that the IP address is responding.*

5.9.8.1. Adding LDAP Groups

Once you have defined users and passwords via your LDAP server, and assigned users to LDAP Groups, you must then grant command and port access rights to each LDAP Group at each individual RPC unit. In order to Add an LDAP Group, you must access the RPC command mode using a password that permits Administrator Level commands. The Add LDAP Group menu allows the following to be defined:

- **Group Name:** Note that this name must match the LDAP Group names that you have assigned to users at your LDAP server. (Default = undefined.)
- **Access Level:** Sets the command access level to either Administrator, SuperUser, User or ViewOnly. For more information on Access Levels, please refer to Section 5.4.1. (Default = User.)
- **Port Access:** Enables/disables this LDAP Group's access to the serial Console Port. (Default = Disabled.)
- **Circuit Access:** Determine which circuits members of this group will be allowed to control. (Default = All Circuits Off.)
- **Circuit Group Access:** Determines which circuit groups the members of this LDAP Group will be allowed to control. (Default = undefined.)
- **Service Access:** Determines whether members of this LDAP group will be allowed to access command mode via the serial Console Port, via Telnet/SSH or via both methods. (Default = Serial Port = On, Telnet/SSH = On, Web = On.)

Note: *After you have defined LDAP Group parameters, make certain to save changes before proceeding. In the Web Browser Interface, click on the "Add LDAP Group" button to save parameters; in the Text Interface, press the* ***[Esc]*** *key several times until the RPC displays the "Saving Configuration" message.*

5.9.8.2 Viewing LDAP Groups

If you need to examine an existing LDAP group definition, the "View LDAP Groups" function can be used to review the group's parameters and Circuit Access Settings.

5.9.8.3. Modifying LDAP Groups

If you want to modify an existing LDAP Group in order to change parameters or circuit access rights, the "Modify LDAP Group" function can be used to reconfigure group parameters. To Modify an existing LDAP Group, you must access the RPC command mode using a password that permits access to Administrator Level commands. Once you have accessed the Modify LDAP Group menu, use the menu options to redefine parameters in the same manner that is used for the Add LDAP Group menu, as discussed in Section 5.9.8.1.

> **Note:** *After you have finished modifying LDAP Group parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Modify LDAP Group" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RPC displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.9.8.4. Deleting LDAP Groups

The Delete LDAP Group function is used to delete LDAP Groups that are no longer in use. In order to Delete an existing LDAP Group, you must access the RPC command mode using a password that permits access to Administrator Level commands.

5.9.9. TACACS Parameters

The TACACS Configuration Menus offer the following options:

- **Enable:** Enables/disables the TACACS feature at the Network Port. (Default = Off.)
- **Primary Address:** Defines the IP address or domain name (up to 64 characters) for your primary TACACS server. (Default = undefined.)
- **Secondary Address:** Defines the IP address or domain name (up to 64 characters) for your secondary, fallback TACACS server (if present.) (Default = undefined.)
- **Secret Word:** Defines the shared TACACS Secret Word for both TACACS servers. (Default = undefined.)
- **Fallback Timer:** Determines how long the RPC will continue to attempt to contact the primary TACACS Server before falling back to the secondary TACACS Server. (Default = 15 Seconds.)
- **Fallback Local:** Determines whether or not the RPC will fallback to its own password/username directory when an authentication attempt fails. When enabled, the RPC will first attempt to authenticate the password by checking the TACACS Server; if this fails, the RPC will then attempt to authenticate the password by checking its own internal username directory. This parameter offers three options:
  - **Off:** Fallback Local is disabled (Default.)
  - **On (All Failures):** Fallback Local is enabled, and the unit will fallback to it's own internal user directory when it cannot contact the TACACS Server, or when a password or username does not match the TACACS Server.
  - **On (Transport Failure):** Fallback Local is enabled, but the unit will only fallback to it's own internal user directory when it cannot contact the TACACS Server.
- **Authentication Port:** The port number for the TACACS function. (Default = 49.)
- **Default User Access:** When enabled, this parameter allows TACACS users to access the RPC command mode without first defining a TACACS user account on the RPC. When new TACACS users access the RPC command mode, they will inherit the default Access Level, Port Access, Circuit Access, Circuit Group Access and Service Access parameters that are defined via the items listed below: (Default = On.)
  - **Enable:** Enables/disables the Default User Access function. (Default = On.)
  - **Access Level:** Determines the default Access Level setting for new TACACS users. This option can set the default access level for new TACACS users to "Administrator", "SuperUser", "User" or "ViewOnly." For more information on Command Access Levels, please refer to Section 5.4.1 and Section 17.2. (Default = User.)
  - **Port Access:** Determines the default Port Access setting for new TACACS users. The Port Access setting determines whether or not the account will be allowed to connect to the serial Console Port. (Defaults; Administrator and SuperUser = Always Enabled, User = Disabled.)

  Note: *ViewOnly level accounts cannot be granted access to the Console Port.*

➤ **Circuit Access:** Determines the default Circuit Access setting for new TACACS users. (Defaults; Administrator and SuperUser = All Circuits On, User = All Circuits Off, ViewOnly = All Circuits Off)

Notes:

- *Administrator and SuperUser level accounts always have access to all circuits.*
- *User level accounts will only have access to the circuits that are defined via the "Circuit Access" parameter.*
- *ViewOnly accounts are not allowed to invoke switching and reboot commands.*

➤ **Circuit Group Access:** Determines the default Circuit Group Access setting for new TACACS users. For more information on Circuit Groups, please refer to Section 5.6. (Defaults; Administrator and SuperUser = All Circuit Groups On, User = All Circuit Groups Off, ViewOnly = All Circuit Groups Off)

Notes:

- *In order to use this feature, Circuit Groups must first be defined as described in Section 5.6.*
- *Administrator and SuperUser level accounts will always have access to all circuit groups.*
- *User Level accounts will only have access to the circuit groups that are defined via the Circuit Group Access parameter.*
- *ViewOnly accounts are not allowed to invoke switching and reboot commands.*

➤ **Service Access:** Selects the default Service Access setting for new TACACS users. The Service Access setting determines whether each account will be able to access command mode via Serial Port, Telnet/SSH or Web. For example, if Telnet/SSH Access is disabled for an account, then the account will not be able to access command mode via Telnet or SSH. (Default = Serial Port = On, Telnet/SSH = On, Web = On)

- **Ping Test:** Allows you to ping IP addresses or domain names that have been defined via the TACACS Parameters menus in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping any user defined IP address in order to make certain that the IP address is responding.*

5.9.10. RADIUS Parameters

In the Text Interface, the RADIUS Parameters menu is accessed via the Network Configuration menu (/N for IPv4 parameters or /N6 for IPv6 parameters.) In the Web Browser Interface, both IPv4 and IPv6 parameters are defined via a single RADIUS Parameters menu, which is accessed via the flyout menus under the Network Configuration link. The RADIUS Configuration Menus offer the following options:

- **Enable:** Enables/Disables the RADIUS feature at the Network Port. (Default = Off)
- **Primary Address IPv4:** Defines the IP address or domain name for your primary RADIUS server when IPv4 protocol is used. (Default = undefined)
- **Primary Address IPv6:** Defines the IP address or domain name for your primary RADIUS server when IPv6 protocol is used. (Default = undefined)
- **Primary Secret Word:** Defines the RADIUS Secret Word for the primary RADIUS server. (Default = undefined)
- **Secondary Address IPv4:** Defines the IP address or domain name for your secondary, fallback RADIUS server when IPv4 protocol is used. (Default = undefined)
- **Secondary Address IPv6:** Defines the IP address or domain name for your secondary, fallback RADIUS server when IPv6 protocol is used. (Default = undefined)
- **Secondary Secret Word:** Defines the RADIUS Secret Word for the secondary RADIUS server. (Default = undefined)
- **Fallback Timer:** Determines how long the RPC will continue to attempt to contact the primary RADIUS Server before falling back to the secondary RADIUS Server. (Default = 3 Seconds)
- **Fallback Local:** Determines whether or not the RPC will fallback to its own password/username directory when an authentication attempt fails. When enabled, the RPC will first attempt to authenticate the password by checking the RADIUS Server; if this fails, the RPC will then attempt to authenticate the password by checking its own internal username directory. This parameter offers three options:
  - **Off:** Fallback Local is disabled (Default.)
  - **On (All Failures):** Fallback Local is enabled, and the unit will fallback to it's own internal user directory when it cannot contact the Radius Server, or when a password or username does not match the Radius Server.
  - **On (Transport Failure):** Fallback Local is enabled, but the unit will only fallback to it's own internal user directory when it cannot contact the Radius Server.
- **Retries:** Determines how many times the RPC will attempt to contact the RADIUS server. Note that the retries parameter applies to both the Primary RADIUS Server and the Secondary RADIUS Server. (Default = 3)
- **Authentication Port:** The Authentication Port number for the RADIUS function. (Default = 1812)

- **Accounting Port:** The Accounting Port number for the RADIUS function. (Default = 1813)
- **Debug:** (Text Interface Only) When enabled, the RPC will put RADIUS debug information into Syslog. (Default = Off)
- **One Time Auth:** This feature should be enabled when using Two Factor Authentication with the One Time Password scheme enabled. When enabled, the One Time Password will be valid for the time specified under the OneTime Auth Timer parameter. (Default = Off)
- **One Time Auth Timer:** When the OneTime Auth parameter is enabled, this parameter determines how long (in minutes) the One Time Password will be valid. (Default = 5 Minutes)
- **Ping Test:** Allows you to ping IP addresses or domain names that have been defined via the RADIUS Parameters menus in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping any user defined IP address in order to make certain that the IP address is responding.*

5.9.10.1. Dictionary Support for RADIUS

The RADIUS dictionary file can allow you to define users and assign command access rights and circuit access rights from a central location. The RADIUS dictionary file, "dictionary.wti" is included on the CDROM along with this user's guide. To install the dictionary file on your RADIUS server, please refer to the documentation provided with your server; some servers will require the dictionary file to reside in a specific directory location, others will require the dictionary file to be appended to an existing RADIUS dictionary file. The WTI RADIUS dictionary file provides the following commands: .

- **`WTI-Super`** - Sets the command access level for the user. This command provides the following arguments:

  `0` = ViewOnly
  `1` = User
  `2` = SuperUser
  `3` = Administrator

  For example, to set the access level to "SuperUser", the command line would be:

  `WTI-Super="2"`

- **`WTI-Plug-Access`** - Determines which circuit(s) the user will be allowed to access. This command provides an argument that consists of a character string, with one character for each the RPC's switched circuits. The following options are available:

  `0` = Off (Deny Access)
  `1` = On (Allow Access)

  For example, to allow access to Circuits 2 and 4, the command line would be:

  `WTI-Plug-Access="0101"`

- **`WTI-Group-Access`** - Determines which circuit group(s) the user will be allowed to access. The argument for this command includes a character for each, defined circuit group. The first character in the string is used to represent the first circuit group defined, and the last character in the string represents the last circuit group defined. The following options are available for each circuit group:

  `0` = Off (Deny Access)
  `1` = On (Allow Access)

  For example, to allow access to the first three defined circuit groups out of a total of six defined circuit groups, the command line would be:

  `WTI-Group-Access="111000"`

Example:
The following command could be used to set the command access level to "User", allow access to Circuits 1 and 2, and also allow access to the first two of five defined circuit groups:

```
tom  Auth-Type:=Local, User-Password=="tom1"
   Login-Service=Telnet,
   Login-TCP-Port=Telnet,
   User-Name="HARRY-tom",
   WTI-Super="1",
   WTI-Circuit-Access="11000000",
   WTI-Group-Access="11000",
```

5.9.11. Email Messaging Parameters

The Email Messaging menu is used to define parameters for email messages that the RPC can send to notify you when an alarm is triggered. To define email message parameters, access the RPC Command Mode using a password that permits access to Administrator Level commands and then proceed as follows:

- **Text Interface:** Type **/N** (for IPv4 parameters) or /N6 (for IPv6 parameters) and press **[Enter]** to access the Network Configuration Menu. Key in the number for the Email Messaging option and press **[Enter]** to display the Email Messaging Menu.
- **Web Browser Interface:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears select either the link for IPv4 parameters or IPv6 parameters to display the Email Messaging Menu.

The Email Configuration menu offers the following options:

- **Enable:** Enables/Disables the Email Messaging feature. When disabled, the RPC will not be able to send email messages when an alarm is generated. (Default = On)
- **SMTP Server:** This prompt is used to define the address of your SMTP Email server. (Default = undefined)
- **Port Number:** Selects the TCP/IP port number that will be used for email connections. (Default = 25)
- **Domain:** The domain name for your email server. (Default = undefined)

  Note: *In order to use domain names, you must first define Domain Name Server parameters as described in Section 5.9.5.*
- **User Name:** The User Name that will be entered when logging into your email server. (Default = undefined)
- **Password:** The password that will be used when logging into your email server. (Default = undefined)
- **Auth Type:** The Authentication type; the RPC allows you to select None, Plain, Login, or CRAM-MD5 Authentication. (Default = Plain)
- **From Name:** The name that will appear in the "From" field in email sent by the RPC. (Default = undefined)
- **From Address:** The email address that will appear in the "From" field in email sent by the RPC. (Default = undefined)
- **To Address:** The address(es) that will receive email messages generated by the RPC. Note that up to three "To" addresses may be defined, and that when Alarm Configuration parameters are selected as described in Section 7, you may then designate one, two or all three of these addresses as recipients for email messages that are generated by the alarms. (Default = undefined)
- **Send Test Email:** Sends a test email, using the parameters that are currently defined for the Email configuration menu.

5.10. Save User Selected Parameters

It is strongly recommended to save all user-defined parameters to an ASCII file as described in Section 15. This will allow quick recovery in the event of accidental deletion or reconfiguration of port parameters.

When changing configuration parameters via the Text Interface, make certain that the RPC has saved the newly defined parameters before exiting from command mode. To save parameters, press the **[Esc**] key several times until you have exited from all configuration menus and the RPC displays the "Saving Configuration" menu and the cursor returns to the command prompt. If newly defined configuration parameters are not saved prior to exiting from command mode, then the RPC will revert to the previously saved configuration after you exit from command mode.

5.10.1. Restore Configuration

If you make a mistake while configuring the RPC unit, and wish to return to the previously saved parameters, the Text Interface's "Reboot System" command (`/I`) offers the option to reinitialize the unit using previously backed up parameters. This allows you to reset the unit to previously saved parameters, even after you have changed parameters and saved them.

Notes:

- *The RPC will automatically backup saved parameters once a day, shortly after Midnight. This configuration backup file will contain only the most recently saved RPC parameters, and will be overwritten by the next night's daily backup.*
- *When the /I command is invoked, a submenu will be displayed which offers several Reboot options. Option 5 is used to restore the configuration backup file. The date shown next to option 5 indicates the date that you last changed and saved unit parameters.*
- *If the daily automatic configuration backup has been triggered since the configuration error was made, and the previously saved configuration has been overwritten by newer, incorrect parameters, then this function will not be able to restore the previously saved (correct) parameters.*

To restore the previously saved configuration, proceed as follows:

1. Access command move via the Text Interface, using a username/password that permits access to Administrator level commands (see Section 5.1.1.)
2. At the RPC command prompt, type `/I` and press **[Enter]**. The RPC will display a submenu that offers several different reboot options.
3. At the submenu, choose Item 5 (Reboot & Restore Last Known Working Configuration. Key in the number for the desired option, and then press **[Enter]**.
4. The RPC will reboot and previously saved parameters will be restored.

6. Reboot Options

In addition to performing reboot cycles in response to commands, the RPC can also be configured to automatically reboot circuits when an attached device does not respond to a Ping command (Ping-No-Answer Reboot) or according to a user defined schedule (Scheduled Reboot.)

- **Ping-No-Answer Reboot:** When the Ping-No-Answer feature is enabled, the RPC will Ping a user selected IP address at regular intervals. If the IP address does not respond to the Ping command, the RPC will reboot one or more user selected circuit(s). Typically, this feature is used to reboot devices when they cease to respond to the Ping command.
- **Scheduled Reboot:** A scheduled reboot is used to initiate a reboot cycle at a user selected time and day of the week. When properly configured and enabled, the RPC will reboot one or more circuits on a daily or weekly basis. The Scheduled Reboot feature can also be used to switch circuit(s) Off at a user selected time, and then switch them back On again at a later, user selected time.

This section describes the procedure for configuring and enabling Ping-No-Answer Reboots and Scheduled Reboots.

> **Note:** *When defining parameters via the Text Interface, make certain to press the **[Esc]** key to completely exit from the configuration menus and save newly defined parameters. When parameters are defined via the Text Interface, newly defined parameters will not be saved until the "Saving Configuration" message is displayed.*

6.1. Ping-No-Answer Reboot

A Ping-No-Answer Reboot can be used to reboot one or more circuits when an attached device does not respond to a Ping Command. In addition, the Ping-No-Answer Reboot feature can also be configured to send an email, Syslog Message or SNMP Trap to notify you whenever a Ping-No-Answer Reboot occurs. Please refer to Section 7.4 for instructions on setting up email alarm notification for Ping-No-Answer reboots.

To set up a Ping-No-Answer Reboot, you must access command mode using a password that permits Administrator level commands. In the Text Interface, the Ping-No-Answer configuration menu is accessed via the Reboot Options menu (/RB). In the Web Browser Interface, the Ping-No-Answer configuration menu is accessed via the Reboot Options link. The Ping-No-Answer configuration menu can be used to Add, Modify, View or Delete Ping-No-Answer Reboot functions.

Note: *In order for the Ping-No-Answer Reboot feature to work properly, your network and/or firewall, as well as the device at the target IP address must be configured to allow ping commands.*

6.1.1. Adding Ping-No-Answer Reboots

Up to 54 Ping-No-Answer Reboots can be defined. The Add Ping-No-Answer menu is used to define the following parameters for each new Ping-No-Answer Reboot:

- **IP Address or Domain Name:** The IP address or Domain Name for the device that you wish to Ping. When the device at this address fails to respond to the Ping command, the RPC will reboot the selected circuits. (Default = undefined)

  Notes:

  - *In order to use domain names, DNS Server parameters must first be defined as described in Section 5.9.5.*
  - *In the Text Interface, a submenu will be displayed that allows the user to choose either IPv4 protocol or IPv6 protocol.*
  - *In the Web Browser Interface, the Add Ping-No-Answer Reboot menu includes a menu item that is used to select IPv4 protocol or IPv6 protocol.*

- **Protocol:** (Web Interface Only) Allows definition of an IPv4 format IP Address or an IPv6 format IP Address. Note that if desired, both an IPv4 and an IPv6 format IP Address may be defined. (Default = IPv4)

- **Ping Interval:** Determines how often the Ping command will be sent to the selected IP Address. The Ping Interval can be any whole number, from 1 to 3,600 seconds. (Default = 60 Seconds)

  Note: *If the Ping Interval is set lower than 20 seconds, it is recommended to define the "IP Address or Domain Name" parameter using an IP Address rather than a Domain Name. This ensures more reliable results in the event that the Domain Name Server is unavailable.*

- **Interval After Failed Ping:** Determines how often the Ping command will be sent after a previous Ping command receives no response. (Default = 10 Seconds.)
- **Ping Delay After PNA Action:** Determines how long the RPC will wait to send additional Ping commands, after a Ping-No-Answer Reboot has been initiated. Typically, this option is used to allow time for a device to fully "wake up" after a Ping-No-Answer Reboot before attempting to Ping the device again. (Default = 15 Minutes.)
- **Consecutive Failures:** Determines how many consecutive failures of the Ping command must be detected in order to initiate a Ping-No-Answer Reboot. For example, if this value is set to "3", then after three consecutive Ping failures, a Ping-No-Answer Reboot will be performed. (Default = 5.)
- **Reboot:** Enables/Disables the Ping-No-Answer Reboot function for the specified IP address. When this item is disabled, the RPC will not reboot the specified circuit(s) when a Ping-No-Answer is detected. However, the RPC can continue to notify you via Email, Syslog Message and/or SNMP Trap, providing that parameters for these functions have been defined as described in Section 5.9 and email notification for the Ping-No-Answer function has been enabled as described in Section 7.4. (Default = No.)

  Notes:

  - *In order for Email/Text Message Notification to function, you must first define Email/Text Message parameters as described in Section 5.9.11.*
  - *In order for Syslog Message Notification to function, you must first define a Syslog Address as described in Section 5.9.2.*
  - *In order for SNMP Trap Notification to function, you must first define SNMP parameters as described in Section 5.9.7.*

- **PNA Action:** Determines how the RPC will react when the IP address fails to respond to a ping. The RPC can either continuously reboot the specified circuit(s) and send notification until the IP address responds and the Ping-No-Answer Reboot is cleared (Continuous Alarm/Reboot), or the RPC can reboot the specified circuit(s) and send notification only once each time the Ping-No-Answer Reboot is initially triggered (Single Alarm/Reboot.) (Default = Continuous Alarm/Reboot.)
- **Circuit Access:** Determines which circuit(s) will be rebooted when the IP address for this Ping-No-Answer operation does not respond to a Ping command. Note that in the Text Interface, Circuit Access is defined via a separate submenu; in the Web Browser Interface, Circuit Access is defined via a drop down menu, accessed by clicking on the "plus" sign in the "Configure Circuit Access" field. (Default = undefined.)
- **Circuit Group Access:** Determines which Circuit Group(s) the Ping-No-Answer Reboot for this IP Address will be applied to. Note that in the Text Interface, Circuit Group Access is defined via a separate submenu; in the Web Browser Interface, Circuit Group Access is defined via a drop down menu, which may be accessed by clicking on the "plus" sign. (Default = undefined.)

- **Ping Test:** (Ping PNA Address) Sends a test Ping command to the IP Address defined for this Ping-No-Answer Reboot.

Notes:

- *In order for the Ping Test function to work properly, your network and/or firewall as well as the device at the target IP address must be configured to allow ping commands.*
- *After you have finished defining or editing Ping-No-Answer Reboot parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add Ping No Answer" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the MPC displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.1.2. Viewing Ping-No-Answer Reboot Profiles

After you have defined one or more Ping-No-Answer Reboot profiles, you can review the parameters selected for each profile using the View Ping-No-Answer feature. In order to view the configuration of an existing Ping-No-Answer profile, you must access command mode using a password that allows Administrator level commands and then use the Ping-No-Answer menu's "View/Modify Ping-No-Answer" function.

6.1.3. Modifying Ping-No-Answer Reboot Profiles

After you have defined a Ping-No-Answer profile, you can modify the configuration of the profile using the Modify Ping-No-Answer feature. In order to modify the configuration of an existing Ping-No-Answer profile, you must access the command mode using a password that allows Administrator level commands and then use the Ping-No-Answer menu's "View/Modify Ping-No-Answer" function.

The RPC will display a screen which allows you to modify parameters for the selected Ping-No-Answer Reboot Profile. Note that this screen functions identically to the Add Ping-No-Answer Reboot menu, as discussed in Section 6.1.1.

Note: *After you have finished defining or editing Ping-No-Answer Reboot parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Change Ping No Answer" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RPC displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.1.4. Deleting Ping-No-Answer Reboot Profiles

After you have defined one or more Ping-No-Answer profiles, you can delete profiles that are no longer needed using the Delete Ping-No-Answer feature. In order to delete an existing Ping-No-Answer profile, you must access the command mode using a password that allows Administrator level commands and then use the Ping-No-Answer menu's "Delete Ping-No-Answer" function.

6.2. Scheduled Reboot

The Scheduled Reboot feature can be used to reboot one or more circuits according to a user-defined schedule, or to automatically turn circuits Off and then On according to a user defined schedule.

In order to configure a Scheduled Reboot, you must access command mode using a password that permits access to Administrator level commands. In the Text Interface, the Scheduled Reboot configuration menu is accessed via the Reboot Options menu (/RB). In the Web Browser Interface, the Scheduled Reboot configuration menu is accessed via the Reboot Options link. The Scheduled Reboot configuration menu can be used to Add, Modify, View or Delete Scheduled Reboot functions.

> **Note:** *After you have finished defining or editing Scheduled Reboot parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add Scheduled Reboot" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RPC displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.2.1. Adding Scheduled Reboots

The RPC allows up to 54 Scheduled Reboots to be defined. The Add Scheduled Reboot menu allows you to define the following parameters for each new Scheduled Reboot:

- **Scheduled Reboot Name:** Assigns a name to this Scheduled Reboot. (Default = undefined.)
- **Circuit Action:** Determines whether the Scheduled Reboot will result in the circuit(s) being switched Off, or cycled Off and then On again (Reboot.) Note that when "Off" is selected, the "Day On" option and the "Time On" option can be used to select a time and day when the circuit(s) will be switched back On again. (Default = Off.)
- **Time:** Determines the time of the day that this Scheduled Reboot will occur on. (Default = 12:00.)
- **Day Access:** This prompt provides access to a submenu which is used to determine which day(s) of the week this Scheduled Reboot will be performed. The Day Access parameter can also be used to schedule a daily reboot; to schedule a daily reboot, use the Day Access submenu to select every day of the week. (Default = undefined.)

  > **Note:** *If you wish to Schedule the RPC to switch an circuit On at one time and then switch the circuit Off at another time, you must define two separate scheduled actions. The first action would be used to switch the circuit On, and the second action would be used to switch the circuit Off.*

- **Circuit Access:** Determines which circuit(s) this Scheduled Reboot action will be applied to. In the Text Interface, circuits are selected by typing 9, pressing [Enter] and then following the instructions in the resulting submenu. In the Web Browser Interface, circuits are designated by clicking on the "plus" sign in the Circuit Access field, and then selecting the desired circuits from the drop down menu. (Default = undefined.)
- **Circuit Group Access:** Determines which Circuit Group(s) this Scheduled Reboot action will be applied to. Note that in the Text Interface, Circuit Group Access is defined via a separate submenu; in the Web Browser Interface, Circuit Group Access is defined via a drop down menu, which may be accessed by clicking on the "plus" sign in the Circuit Group Access field. (Default = undefined.)

6.2.2. Viewing Scheduled Reboot Actions

After you have defined one or more Scheduled Reboots, you can review the parameters selected for each Reboot using the View Scheduled Reboot feature. In order to view the configuration of an existing Scheduled Reboot, you must access the command mode using a password that allows Administrator level commands and then use the Scheduled Reboot menu's "View/Modify Scheduled Reboot" function.

The RPC will display a screen which lists all defined parameters for the selected Scheduled Reboot action.

6.2.3. Modifying Scheduled Reboots

After you have defined a Scheduled Reboot, you can edit the configuration of the Reboot action using the Modify Scheduled Reboot feature. In order to modify the configuration of an existing Scheduled Reboot action, you must access the command mode using a password that allows Administrator level commands and then use the Scheduled Reboot menu's "View/Modify Scheduled Reboot" function.

The RPC will display a screen which allows you to modify parameters for the selected Scheduled Reboot action. Note that this screen functions identically to the Add Scheduled Reboot menu, as discussed in Section 6.2.1.

6.2.4. Deleting Scheduled Reboots

After you have defined one or more Scheduled Reboot actions, you can delete Reboot actions that are no longer needed using the Delete Scheduled Reboot feature. In order to delete an existing Scheduled Reboot, access the command mode using a password that allows Administrator level commands and then use the Scheduled Reboot menu's "Delete Scheduled Reboot" function.

7. Alarm Configuration

When properly configured, RPC units can monitor rack temperature, ping command response and other factors at network installation sites.

If user defined trigger levels for temperature are exceeded, the RPC can also perform load shedding; automatically shutting off user-designated power circuits in order to reduce the amount of heat generated in the rack. When temperatures return to acceptable levels, the RPC can then switch circuits back on again. When any of the user-defined alarms are triggered, the RPC can send an alarm message to the proper personnel via Email, Syslog Message or SNMP trap.

This section describes the procedure for setting up the RPC to send alarm messages when critical situations are detected. For instructions regarding configuration of the Log function, please refer to Section 5.3.3.

Notes:

- *In order to send alarm notification via email, email addresses and parameters must first be defined as described in Section 5.9.11. Email alarm notification will then be sent for all alarms that are enabled as described in this Section.*
- *In order to send alarm notification via Syslog Message, a Syslog address must first be defined as described in Section 5.9.2. Once the Syslog address has been defined, Syslog Messages will be sent for every alarm that is discussed in this Section, providing that the Trigger Enable parameter for the alarm has been set to "On."*
- *In order to send alarm notification via SNMP Trap, SNMP Trap parameters must first be defined as described in Section 5.9.7. Once SNMP Trap Parameters have been defined, SNMP Traps will be sent for every alarm that is discussed in this Section, providing that the Trigger Enable parameter for the alarm has been set to "On."*
- *When defining parameters via the Text Interface, make certain to press the **[Esc]** key to completely exit from the configuration menu and save newly defined parameters. When parameters are defined via the Text Interface, newly defined parameters will not be saved until the "Saving Configuration" message is displayed.*

To configure the RPC Alarm functions, access the command mode using a password that allows Administrator level commands and then activate the Alarm Configuration menu (in the Text Interface, type **/AC** and press **[Enter]**; in the Web Browser Interface, click on the "Alarm Configuration" link.)

7.1. The Over Temperature Alarms

The Over Temperature Alarms are designed to inform you when the temperature level inside your equipment rack reaches or exceeds certain user-defined levels. There are two separate Over Temperature Alarms; the Initial Threshold alarm and the Critical Threshold Alarm.

Typically, the Initial Threshold alarm is used to notify you when the temperature within your equipment rack reaches a point where you *might* want to investigate it, whereas the Critical Threshold alarm is used to notify you when the temperature approaches a level that may harm equipment or inhibit performance. The trigger for the Initial Threshold alarm is generally set lower than the Critical Threshold alarm.

If the user-defined trigger levels for temperature are exceeded, the RPC can automatically shut off power to non-essential devices ("Load Shedding") in order to reduce the amount of temperature that is being generated within the rack. In addition, the Load Shedding feature can also be used to switch On additional components, such as fans or cooling systems in order to dissipate the excess heat. After Load Shedding has taken place, the Load Shedding Recovery feature can be used to return circuits to their previous state after the temperature drops to an acceptable level.

Notes:

- *In order for the unit to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the unit to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the unit to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Over Temperature Alarms, access the RPC command mode using a password that permits Administrator Level commands, and then use the Alarm Configuration menu to select the desired alarm feature.

Both the Initial Threshold menus and Critical Threshold menus offer essentially the same parameters, but the parameters defined for each alarm are separate. Therefore, parameters defined for the Critical Threshold Alarm will not be applied to the Initial Threshold Alarm and vice versa. Both the Over Temperature (Initial Threshold) alarm and the Over Temperature (Critical Threshold) alarm offer the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On.)

Note:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all RPC alarms. For example, if the Over Temperature Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then all other RPC alarms will also be enabled.*

- **Alarm Set Threshold:** The trigger level for this alarm. When temperature exceeds the Alarm Set Threshold, the RPC can send an alarm (if enabled) and/or begin Load Shedding (if enabled.) For more information on Load Shedding for the Over Temperature Alarm, please refer to Section 7.1.1. (Initial Threshold: Default = 90°F or 32°C, Critical Threshold: Default = 100°F or 38°C)

  Note: *The Alarm Set Threshold value must be greater than the Alarm Clear Threshold value. The RPC will not allow you to define an Alarm Clear Threshold value that is higher than the Alarm Set Threshold.*

- **Alarm Clear Threshold:** Determines how low the temperature must drop in order for the Alarm condition to be cancelled and for Load Shedding (if enabled) to occur. For more information on Load Shedding for the Over Temperature Alarm, please refer to Section 7.1.1. (Initial Threshold: Default = 80°F or 27°C, Critical Threshold: Default = 90°F or 38°C.)

  Note: *The System Parameters menu is used to set the temperature format for the RPC unit to either Fahrenheit or Celsius as described in Section 5.3.*

- **Resend Delay:** Determines how long the RPC will wait to resend an email message generated by this alarm, when the initial attempt to send notification was unsuccessful. (Default = 60 Minutes.)

- **Notify Upon Clear:** When this item is enabled, the RPC will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RPC will send initial notification when it detects that the temperature has exceeded the trigger value, and then send a second notification when it determines that the temperature has fallen below the trigger value. (Default = On.)

- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)

- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses, defined via the "Email Messages" menu (see Section 5.9.11,) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

  Note: *If Email addresses have been previously defined, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: Over Temperature (Initial)" or "Alarm: Over Temperature (Critical)".)

- **Load Shedding:** Provides access to a submenu, which is used to configure and enable the Load Shedding feature for the Over Temperature alarms. When Load Shedding is enabled and properly configured, the RPC will switch specific, user-selected circuits On or Off whenever the temperature exceeds the Alarm Set Threshold value. If the Auto Recovery feature is enabled, the RPC can also return these user-selected circuits to their prior status, when the temperature falls below the Alarm Clear Threshold value. For more information on the Load Shedding Feature and Auto Recovery, please refer to Section 7.1.1.

7.1.1. Over Temperature Alarms - Load Shedding and Auto Recovery

For Over Temperature Alarms, the Load Shedding feature is used to switch specific, user-defined circuits On or Off whenever temperature exceeds the Alarm Set Threshold value. This allows the RPC to automatically shut Off non-essential devices in order to reduce the temperature generated within the rack, or automatically switch On devices such as fans or cooling systems in order to dissipate heat. When the Auto Recovery feature is enabled, the RPC can also automatically "undo" the effects of the Load Shedding feature when the temperature again falls to a user-defined non-critical level.

> **Note:** *Load Shedding Configuration Menus for both the Initial and Critical Over Temperature Alarms offer essentially the same set of parameters, but parameters defined for each alarm are separate and unique. For example, parameters defined for Over Temperature (Initial) Alarm Load Shedding will not be applied to Over Temperature (Critical) Alarm Load Shedding and vice versa.*

The Load Shedding Configuration menus allow you to defined the following parameters:

- **Configure Loadshedding for Unit:** In the Text Interface, this item is used to access the Load Shedding parameters listed below. In the Web Browser Interface, Load Shedding parameters are accessed via the "Load Shedding" button in the Temperature Alarm configuration menus.
  - **Enable:** Enables/Disables Load Shedding for the Over Temperature Alarm. When enabled, the RPC will switch the user specified circuits whenever the temperature exceeds the Alarm Set Threshold value. (Default = Disable.)
  - **Circuit State:** Determines whether the selected circuits/circuit groups will be switched On or Off when Load Shedding is enabled and temperature exceeds the user-defined Alarm Set Threshold. For example, if the Circuit State is set to "Off", then the selected circuits/circuit groups will be switched Off when the Alarm Set Threshold is exceeded. (Default = Off.)
  - **Auto Recovery:** Enables/Disables the Auto Recovery feature for the selected unit. When both Load Shedding and Auto Recovery are enabled, the RPC will return circuits to their former On/Off state after the temperature falls below the Alarm Clear Threshold value. This allows the RPC to "undo" the effects of the Load Shedding feature after the temperature returned to an acceptable level. (Default = Off.)
  - **Circuit Access:** Determines which Circuit(s) will be switched when the temperature exceeds the Alarm Set Threshold and Load Shedding is triggered. For example, if circuits A1, A2 and A3 are selected, these circuits will be switched On or Off whenever the temperature exceeds the Alarm Set Threshold. (Default = undefined.)

Notes:

- *In the Text Interface, Circuit Access is configured by typing* **4***, pressing* ***[Enter]*** *and then selecting the desired Circuit(s) from the resulting submenu.*
- *In the Web Browser Interface, Circuit Access is configured by clicking on the "plus" symbol in the "Configure Circuit Access" field to display the drop down menu, and then selecting the desired Circuit(s) from the drop down menu.*

- **Circuit Group Access:** Determines which Circuit Group(s) will be switched when the Load Shedding feature is triggered. (Default = undefined.)

Notes:

- *Circuit Groups must first be defined (as described in Section 5.6) before they will be displayed in the Load Shedding menu's Circuit Group Access submenu.*
- *In the Text Interface, Circuit Group Access is configured by typing* **5**, *pressing* ***[Enter]*** *and then selecting the desired Circuit Group(s) from the resulting submenu.*
- *In the Web Browser Interface, Circuit Group Access is configured by clicking on the "plus" symbol in the "Configure Circuit Group Access" field to display the drop down menu, and then selecting the desired Circuit Group(s) from the drop down menu.*

7.2. The Circuit Breaker Open Alarm (RPC-40L8A4 Series Units Only)

The Circuit Breaker Alarm is intended to provide notification in the event that one of the RPC-40L8A4 series unit's fuse is blown. When a fuse is blown, the RPC-40L8A4 can provide prompt notification via Email, Syslog Message or SNMP Trap.

Notes:

- *The Circuit Breaker Open Alarm is not available on RPC-4850 series units.*
- *In order for the RPC-40L8A4 to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RPC-40L8A4 to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the RPC-40L8A4 to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Circuit Breaker Alarm, you must access the RPC-40L8A4 command mode using a password that permits Administrator Level commands. The Circuit Breaker Open Alarm Configuration Menu offers the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On)

Note:

- *When an alarm is generated, to cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all RPC-40L8A4 alarms. For example, if the Circuit Breaker Open Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then all other RPC-40L8A4 alarms will also be enabled.*

- **Resend Delay:** Determines how long the RPC-40L8A4 will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes)
- **Notify Upon Clear:** When this item is enabled, the unit will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the unit can send initial notification when it detects a blown fuse, and then send a second notification when it determines that the fuse has been replaced. (Default = On)
- **Email Message:** Enables/Disables email notification for this alarm. (Default = On)

- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On)

  Note: *If Email addresses have been previously defined, then the text under the parameters will list the current, user selected email addresses.*

- **Subject:** Defines the text that will appear in the "Subject" field for email notification messages generated by this alarm. (Default = "Alarm: Circuit Breaker Open")

7.3. The Lost Voltage (Line In) Alarm (RPC-40L8A4 Series Units Only)

The Lost Voltage (Line In) Alarm can provide notification after the power supply to the RPC-40L8A4 unit has been interrupted.

Notes:

- *The Lost Voltage Alarm is not available on RPC-4850 series units.*
- *The Lost Voltage (Line In) alarm will provide notification when one of the available power supplies is lost or disconnected. This alarm will not function if all input power to the RPC-40L8A4 unit is lost. To provide notification when all input power is lost and restored, please use the Power Cycle Alarm as described in Section 7.6.*
- *In order for the RPC-40L8A4 to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RPC-40L8A4 to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the RPC-40L8A4 to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Lost Voltage (Line In) Alarm, you must access the RPC-40L8A4 command mode using a password that permits Administrator Level commands. The Lost Voltage Alarm Configuration menu offers the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On)

Note:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all RPC-40L8A4 alarms. For example, if the Lost Voltage Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then all other RPC-40L8A4 alarms will also be enabled.*

- **Resend Delay:** Determines how long the RPC-40L8A4 will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes)
- **Notify Upon Clear:** When enabled, the RPC-40L8A4 will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RPC-40L8A4 will send initial notification when it detects that one of it's power supplies has been lost or disconnected, and then send a second notification when it determines that power has been restored. (Default = On)

- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)
- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

  Note: *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: Lost Voltage (Line In)")

7.4. The Ping-No-Answer Alarm

The Ping-No-Answer Alarm is intended to provide notification when one of the IP addresses defined via the Ping-No-Answer Reboot feature (described in Section 6.1) fails to respond to a Ping command. When one of the user-defined IP addresses fails to answer a Ping command, the RPC can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for the Ping-No-Answer Alarm to work properly, your network and/or firewall, as well as the device at the target IP address, must be configured to allow ping commands.*
- *In order for this alarm to function, IP Addresses for the Ping-No-Answer reboot feature must first be defined as described in Section 6.1.*
- *When a Ping-No-Answer condition is detected, the RPC can still reboot the user-selected circuit(s) as described in Section 6.1, and can also send an email, Syslog Message and/or SNMP trap as described in this section.*
- *In order for the RPC to provide Email alarm notification, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RPC to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the RPC to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Ping-No-Answer Alarm, you must access the RPC command mode using a password that permits Administrator Level commands. The Ping-No-Answer alarm configuration menu offers the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On.)

Note:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all RPC alarms. For example, if the Ping-No-Answer Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then all other RPC alarms will also be enabled.*

- **Resend Delay:** Determines how long the RPC will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes.)

- **Notify Upon Clear:** When this item is enabled, the RPC will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RPC will send initial notification when it detects that a Ping command has failed, and then send a second notification when it determines that the IP address is again responding to the Ping command. (Default = On.)
- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)
- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

  Note: *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages that are generated by this alarm. (Default = "Alarm: Ping-No-Answer")

7.5. The Serial Port Invalid Access Lockout Alarm

The Serial Port Invalid Access Lockout Alarm can provide notification when the RPC has locked the serial Console Port due to repeated, invalid attempts to access command mode. Normally, the Invalid Access Lockout feature (discussed in Section 5.3.2) can lock the serial Console Port whenever the unit detects that a user-defined threshold for invalid access attempts at the Console Port is exceeded. When a serial port lockout occurs, the unit can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *Note that Serial Port Invalid Access Lockout Alarm is only intended to provide notification when the Invalid Access Lockout feature has locked the serial Console Port. To apply the Invalid Access Lockout feature to SSH, Telnet or Web access, please refer to Section 5.3.2.*
- *In order for this alarm to function, Invalid Access Lockout parameters for the serial port must first be configured and enabled as described in Section 5.3.2.*
- *If desired, the RPC can be configured to count Invalid Access attempts at the serial Console port, and provide notification when the counter exceeds a user defined trigger level, without actually locking the port in question. To do this, enable the Invalid Access Lockout Alarm as described here, but when you configure Invalid Access Lockout parameters as described in Section 5.3.2, set the Lockout Attempts and Lockout Duration as you would normally, and then set the "Lockout Enable" parameter to "Off."*
- *In order for the RPC to provide Email alarm notification, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RPC to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the RPC to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Serial Port Invalid Access Lockout Alarm, you must access the RPC command mode using a password that permits Administrator Level commands. The Invalid Access Lockout alarm configuration menu offers the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On.)

Note:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify on Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all RPC alarms. For example, if the Invalid Access Lockout Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then other RPC alarms will also be enabled.*

- **Resend Delay:** Determines how long the RPC will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes.)
- **Notify Upon Clear:** When this item is enabled, the RPC will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RPC will send initial notification when it detects that an Invalid Access Lockout has occurred, and then send a second notification when it determines that the port has been unlocked. (Default = On.)
- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)
- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

  Note: *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: Invalid Access Lockout")

7.6. The Power Cycle Alarm

The Power Cycle Alarm can provide notification when all input power to the RPC unit is lost and then restored. When the power supply is lost and then restored, the RPC can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for the RPC to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RPC to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the RPC to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Power Cycle Alarm, you must access the RPC command mode using a password that permits Administrator Level commands. The Power Cycle Alarm configuration menu offers the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On.)

  Note:

  - *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
  - *The Trigger Enable, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all RPC alarms. For example, if the Power Cycle Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then other RPC alarms will also be enabled.*

- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)
- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

  Note: *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: Power Cycle")

7.7. The Alarm Input Alarm (RPC-40L8A4 Series Units Only)

The Alarm Input Alarm can be used to monitor dry contacts that have been connected to the Alarm Inputs on the RPC-40L8A4's back panel as described in Section 3.2.4. Typically, the Alarm Input Alarm is used to detect open doors and other situations where a dry contact has been opened or closed.

Note: *The Alarm Input Alarm is not available on RPC-4850 Series units.*

To configure the Alarm Input Alarm, you must first connect a dry contact relay to the alarm inputs on the RPC-40L8A4 back panel as described in Section 3.2.4 and then access the RPC-40L8A4 command mode using a password that permits Administrator Level commands. The Power Cycle Alarm configuration menu offers the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On)

  Note:
  - *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
  - *The Trigger Enable, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all RPC-40L8A4 alarms. For example, if the Alarm Input Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then other RPC-40L8A4 alarms will also be enabled.*

- **Resend Delay:** Determines how long the RPC-40L8A4 will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes)

- **Notify Upon Clear:** When this item is enabled, the RPC-40L8A4 will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RPC-40L8A4 will send initial notification when it detects that the Alarm Input Alarm has been triggered, and then send a second notification when it determines that the condition that triggered the alarm has been cleared. (Default = On)

- **Email Message:** Enables/Disables email notification for this alarm. (Default = On)

- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On)

  Note: *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: Power Cycle")
- **Alarm Input Parameters:** Provides access to a submenu that is used to Enable/ Disable the alarm at each Alarm Input, name Alarm Inputs, set trigger levels for each Alarm Input and also select load shedding parameters for each Alarm Input.

Notes:

- *The Alarm Input Alarm must be enabled in order to access the Alarm Input Parameters submenu.*
- ***Text Interface:*** *When accessing the Alarm Input Parameters submenu via the Text Interface, first type* `11` *and press* ***[Enter]*** *to access the first Alarm Input Parameters submenu. From the Alarm Input Parameters submenu, key in the number of the desired Alarm Input and then press* ***[Enter]*** *to display the Alarm Input Parameters submenu for an individual Alarm Input.*
- ***Web Browser Interface:*** *To access the Alarm Input Parameters submenu via the Web Browser Interface, click the Alarm Input Parameters button at the bottom of the Alarm Input configuration menu. In the Web Browser Interface, all Alarm Input Parameters for all four Alarm Inputs may be defined via a single submenu.*

The Alarm Input Parameters submenu will allow you to define the following parameters for each Alarm Input:

- **Name:** Can be used to define a unique name for each Alarm Input. (Default = undefined.)
- **Enable:** Enables/Disables each Alarm Input. (Default = Off)
- **Level:** Defines the trigger level for each Alarm Input as either Open or Closed. For example, if the Level is set to "Open" and the Alarm Input Alarm is properly configured, an alarm will be generated when the dry contact relay connected to the corresponding Alarm Input is Opened. (Default = Open)
- **Load Shedding:** Allow the Alarm Input Alarm to automatically shut off user specified circuits or circuit groups when an Alarm is generated. This feature works identically to the Load Shedding feature in the Over Temperature Alarms. For more information, please refer to Section 7.1.1. (Default = undefined)

7.8. The No Dialtone Alarm

The No Dialtone Alarm enables the RPC to monitor a telephone line connected to an external modem installed at the RPC Console Port, and then provide notification if the RPC detects that the phone line is dead or no dialtone is present.

If the No Dialtone Alarm is enabled and the RPC determines that there is no dialtone signal, the No Dialtone Alarm can provide notification via email using a network connection. In the event that the RPC unit is not connected to a network cable, the RPC will also create an entry in the Alarm Log, indicating that the No Dialtone Alarm has been triggered.

Notes:

- *In order for this alarm to function, the No Dialtone Alarm parameter in the Serial Port Configuration menu must first be configured and enabled as described in Section 5.8.*
- *In order for the RPC to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RPC to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the RPC to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

The configuration menu for the No Dialtone Alarm allows the following parameters to be defined:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On)

Note:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify Upon Clear, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all RPC alarms. For example, if the No Dialtone Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then all other RPC alarms will also be enabled.*

- **Resend Delay:** Determines how long the RPC will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes)

- **Notify Upon Clear:** When this item is enabled, the RPC will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RPC will send initial notification when it detects that the dialtone for the external modem has been lost, and then send a second notification when it determines that the dialtone has been restored. (Default = On)
- **Email Message:** Enables/Disables email notification for this alarm. (Default = On)
- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On)

  Note: *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: No Dial Tone")

8. The Status Screens

The Status Screens are used to display status information about the RPC unit, switched circuits, Network Port and Circuit Groups. The Status Screens are available via both the Text Interface and Web Browser Interface.

8.1. Product Status

The Product Status Screen lists the model number, software version and other information for your RPC unit. To display the Product Status Screen via the Text Interface, type `/J *` and then press **[Enter]**. To display the Product Status Screen via the Web Browser Interface, click on the "Product Status" link.

> **Note:** *The Information provided by the Product Status Screen is intended mainly to assist WTI support peronnel with the diagnosis of user equipment problems.*

8.2. The Network Status Screen

The Network Status screen shows activity at the RPC's 16 virtual network ports. To view the Network Status Screen, you must access command mode using a password that permits access to Administrator Level commands.

To display the Network Status Screen via the Text Interface, type `/SN` and press **[Enter]**. To display the Network Status Screen via the Web Browser Interface, click on the Network Status link.

8.3. The Circuit Status Screen

The Circuit Status screen shows the On/Off status of the RPC's switched circuits, and lists user-defined Circuit Names, Boot/Sequence Delay values, and Default On/Off settings. On RPC-40L8A4 series units, the Circuit Status Screen will also lists the status of the Alarm Inputs.

Notes:

- *When the Circuit Status Screen is viewed by an "Administrator" or "SuperUser" level account, all RPC circuits are listed. When the Circuit Status Screen is viewed by a "User" or "ViewOnly" level account, the screen will list only the circuits that are allowed by that account.*
- *Section 5.7 describes the procedure for configuring the circuit parameters that are listed in the Circuit Status Screen.*
- *The Alarm Inputs are not included on RPC-4850 series units.*

To display the Circuit Status Screen via the Text Interface, type **/S** and press **[Enter]**. To display the Circuit Status Screen via the Web Browser Interface, click on the "Circuit Status" link. Note that when the **/S** command is invoked via the Text Interface, the command line can also include arguements that display On/Off status for an individual circuit, two or more specific circuits, or a range of circuits:

/S Displays configuration details and ON/Off status for all switched circuits.

/S *s* Displays On/Off status for an individual circuit, where ***s*** is the name or number of the desired circuit.

/S *s*+*s* Displays On/Off status for two or more specific circuits, where ***s*** is the number or name of each desired circuit. A plus sign (**+**) is entered between each circuit number or name.

/S *s*:*s* Displays On/Off status for a range of circuits, where ***s*** is the number or name of the circuit at the beginning and end of the range of desired circuits. A colon (**:**) is entered between the two circuit numbers or names that mark the beginning of the range and the end of the range.

8.4. The Circuit Group Status Screen

The Circuit Group Status screen shows the configuration details and On/Off status for the RPC's user-defined Circuit Groups.

Notes:

- *When the Circuit Group Status Screen is viewed by an "Administrator" or "SuperUser" level account, all RPC circuits and circuit groups are listed. When the Circuit Status Screen is viewed by a "User" or "ViewOnly" level account, the screen will list only the circuit groups that are allowed by that account.*
- *In order to display the Circuit Group Status screen, you must first define at least one Circuit Group as described in Section 5.6.*

To display the Circuit Group Status Screen via the Text Interface, type **/SG** and then press **[Enter]**. To display the Circuit Group Status Screen via the Web Browser Interface, click on the "Circuit Group Status" link and then select the desired Circuit Group from the resulting subment and click on the "Get Circuit Group Status" button.

8.5. The Port Diagnostics Screen

The Port Diagnostics Screen provides more detailed information about the RPC's Serial Port. To display the Port Diagnostics Screen, access the Text Interface command mode and type **/SD [Enter]**.

Note: *The Port Diagnostics Screen is only available via the Text Interface.*

8.6. Alias Status Screen

The Alias Status Screen lists user defined IP alias for the RPC's Serial Port.

Note: *The Alias Status Screen is only available via the Text Interface.*

To display the Alias Status Screen via the Text Interface, type **/SA** and press **[Enter]**.

8.7. The Alarm Status Screen

The Alarm Status Screen lists all available user-defined alarms and indicates whether or not each alarm has been triggered. The resulting screen will display "Yes" (or 1) for alarms that have been triggered or "No" (or 0) for alarms that have not been triggered. If desired, the /AS command line can also include an optional alarm argument that will cause the unit to display the status of one individual alarm.

To display the Alarm Status Screen via the Text Interface, type **`/AS`** and press **[Enter]**.

For a list of alarm arguments, please refer to Section 17.3.1.

8.8. The Serial Port Parameters Screen

The /W (Who) command displays more detailed information about the RPC's Serial Port. Rather than listing general connection information, the Port Parameters screen lists all defined parameters for the Serial port. To display the Serial Port Parameters Screen, type **`/W`** and press **[Enter]**.

The /W command uses the following format:

`/W xx` **[Enter]**

Note: *The Serial Port Parameters screen is only available via the Text Interface.*

9. Operation

The RPC offers two separate command interfaces; the Web Browser Interface and the Text Interface. Both interfaces offer essentially the same command options and features, and in most cases, parameters defined via the Web Browser Interface will also apply when communicating via the Text Interface (and vice versa.)

9.1. Operation via the Web Browser Interface

When using the Web Browser Interface, switching commands are invoked via the Circuit Control Screen and Circuit Group Control Screen.

9.1.1. The Circuit Control Screen - Web Browser Interface

The Circuit Control Screen lists the On/Off status of the RPC's Switched Circuits and is used to control switching and rebooting of the circuits. To invoke power switching commands, first access the RPC command mode (for more information, see Section 5.1.) After accessing command mode, click on the "Circuit Control" link on the left hand side of the screen to display the Circuit Control Screen.

When the Circuit Control Screen appears, click the down arrow in the "Action" column for the desired circuit(s), then select the desired switching option from the dropdown menu and click on the "Confirm Circuit Actions" button.

When the "Confirm Circuit Actions" button is pressed, the RPC will display a screen which lists the selected action(s) and asks for confirmation before proceeding. To implement the selected action(s), click on the "Execute Circuit Actions" button. The RPC will display a screen which indicates that a switching operation is in progress, then display the Circuit Status screen when the command is complete. At that time, the Status Screen will list the updated On/Off status of each circuit.

Notes:

- *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 5.7.*
- *If a switching or reboot command is directed to a circuit that is already in the process of being switched or rebooted by a previous command, then the new command will be placed in a queue until the circuit is ready to receive additional commands.*
- *If the Status column in the Circuit Control Screen includes an asterisk, this means that the corresponding circuit is busy completing a previously invoked command.*
- *When the Circuit Control Screen is displayed by an account that permits Administrator or SuperUser level commands, all switched circuits will be displayed.*
- *When the Circuit Control Screen is displayed by a User level account, the screen will only include the switched circuits that are allowed by the account.*

9.1.2. The Circuit Group Control Screen - Web Browser Interface

The Circuit Group Control Screen is used to send switching and reboot commands to the user-defined Circuit Groups. As described in Section 5.6, Circuit Groups allow you to specify a group of circuits that are dedicated to a similar purpose or client, and then direct switching commands to the group, rather than switching one circuit at a time.

To apply power switching commands to Circuit Groups, first access the RPC Command Mode (see Section 5.1.) Click on the "Circuit Group Control" link on the left hand side of the screen to display the Circuit Group Control Screen. When the Circuit Group Control Screen appears, click the down arrow in the "Action" column for the desired Circuit Group(s), then select the desired switching option from the dropdown menu and click on the "Confirm Circuit Actions" button

When the "Confirm Circuit Group Actions" button is pressed, the RPC will display a screen which lists the selected action(s) and asks for confirmation before proceeding. To implement the selected circuit group action(s), click on the "Execute Circuit Group Actions" button. The RPC will display a screen which indicates that a switching operation is in progress, then display the Circuit Status screen when the command is complete. At that time, the Status Screen will list the updated On/Off status of each circuit.

Notes:

- *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 5.7.*
- *If a switching or reboot command is directed to a circuit that is already in the process of being switched or rebooted by a previous command, then the new command will be placed in a queue until the circuit is ready to receive additional commands.*
- *When the Circuit Group Control Screen is displayed by an account that permits Administrator or SuperUser level commands, all user-defined Circuit Groups will be displayed.*
- *When the Circuit Control Screen is displayed by a User level account, the screen will only include the Circuit Groups that are specifically allowed for that account.*

9.2. Operation via the Text Interface

When using the Text Interface, all switching functions are performed by invoking simple, ASCII commands. ASCII commands are also used to display status screens and to log out of command mode. The Text Interface includes a Help Menu, which summarizes all available RPC commands. To display the Text Interface Help Menu, type **`/H`** and press **[Enter]**.

> **Note:** *When the Help Menu is displayed by a SuperUser, User or ViewOnly level account, the screen will not include commands that are only available to Administrator level accounts.*

9.2.1. Switching and Reboot Commands - Text Interface

These commands can be used to switch or reboot the RPC's switched circuits, and can also be used to set circuits to the user-defined Power-Up Default values. Circuits may be specified by name or number.

Notes:

- *If a switching or reboot command is directed to a circuit that is already being switched or rebooted by a previous command, then the new command will be placed in a queue until the circuit is ready to receive additional commands.*
- *If an asterisk appears in the "Status" column for any given circuit, this indicates that the circuit is currently busy, processing a previously issued command.*
- *Commands are not case sensitive. All commands are invoked by pressing* **[Enter]**.
- *When the Circuit Control Screen is displayed by an account that permits Administrator level command access, all switched circuits will be displayed.*
- *When you have accessed command mode using an account that permits Administrator or SuperUser level commands, then switching and reboot commands can be applied to all circuits.*
- *When you have accessed command mode via a User level account, switching and reboot commands can only be applied to the circuits that are specifically allowed for that account.*
- *If command confirmation is enabled, the RPC will display the Status Screen after commands are successfully completed.*
- *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 5.7.*
- *When used in On/Off/Reboot command lines, circuit names and circuit group names are* ***not*** *case sensitive.*

When switching and reboot commands are executed, the RPC will display a "Sure?" prompt, wait for user response, and then complete the command. The unit will pause for a moment while the command is executed, and then return to the Circuit Status Screen. To Switch Circuits, or initiate a Reboot Cycle, proceed as follows:

1. **Switch Circuit(s) On:** Type **/ON *n*** and press **[Enter]**. Where "**n**" is the alphanumeric number or name of the desired circuit or Circuit Group. For example:

   /ON A1 [Enter] or **/ON ROUTER [Enter]**

2. **Switch Circuit(s) Off:** Type **/OFF n** and press **[Enter]**. Where "**n**" is the alphanumeric number or name of the desired circuit or Circuit Group. Note that the "**/OFF**" command can also be entered as "**/OF**". For example:

   /OFF A2 [Enter] or **/OF ROUTER [Enter]**

3. **Reboot Circuit(s):** Type **/BOOT n** and press **[Enter]**. Where "**n**" is the alphanumeric number or name of the desired circuit or Circuit Group. Note that the "**/BOOT**" command can also be entered as "**/BO**". For example:

   /BOOT A3 [Enter] or **/BO ATMSWTCH [Enter]**

4. **Set All Circuits to Power Up Defaults:** Type **/DPL** and press **[Enter]**. All circuits permitted by your account will be set to their default On/Off status, which is defined via the Circuit Parameters Menu as described in Section 5.7.

   Notes:

   - *When you have accessed command mode using an Administrator or SuperUser level account, the Default command will be applied to all circuits.*
   - *When you have accessed command mode using an account that permits only User level command access, the Default command will only be applied to the circuits specifically allowed by that account.*
   - *The /DPL command is not available in ViewOnly mode.*

5. **Suppress Command Confirmation Prompt:** To execute a power switching command without displaying the "Sure?" prompt, include the "**,Y**" option at the end of the command line. For example:

   /ON ROUTER,Y or **/BOOT A2,Y**

9.2.2. Applying Commands to Several Circuits - Text Interface

As described below, switching and reboot commands can be applied to only one Switched AC Circuit, or to an assortment of circuits.

Note: *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 5.7.*

1. **Switch Several Circuits:** To apply a command to several circuits, enter the numbers of the desired circuits, separated by commas or plus signs. For example to switch circuits A1, A3, and A4 Off, enter either of the following commands:

   `/OFF A1+A3+A4` [Enter]
   or
   `/OFF A1,A3,A4` [Enter]

   Note: *In order for the "+" or "," operators to work, there must be no spaces between the circuit name or number and the plus sign or comma.*

2. **Switch a Series of Circuits:** To apply a command to a series of circuits, enter the numbers for the circuits that mark the beginning and end of the series, separated by a colon. For example to switch On circuits A1 through A4 enter the following:

   `/ON A1:A4` [Enter]

3. **All Circuits:** To apply a command to all circuits, enter an asterisk in place of the name or number. For example, to Boot all circuits, enter the following:

   `/BO *` [Enter]

   Note: *When this command is invoked by a User level account, it will only be applied to the circuits that are specifically allowed for that account.*

9.3. The Automated Mode

The Automated Mode allows the RPC to execute switching and reboot commands, without displaying menus or generating response messages. Automated Mode is designed to allow the RPC to be controlled by a device which can generate commands to control power switching functions without human intervention.

When Automated Mode is enabled, the /ON, /OFF, /BOOT, /DPL and /X commands are executed without a "Sure?" confirmation prompt and without command response messages; the only reply to these commands is the command prompt, which is displayed when the command is complete.

Note that although Automated Mode can be enabled using either the Web Browser Interface or Text Interface, Automated Mode is designed primarily for users who wish to send ASCII commands to the RPC without operator intervention, and therefore does not specifically apply to the Web Browser Interface. When Automated Mode is enabled, the Web Browser Interface can still be used to invoke On / Off / Boot commands.

Notes:

- *When Automated Mode is enabled, all RPC password security functions are disabled, and users are able to access System Level command functions (including the configuration menus) and control circuits without entering a password.*
- *If you need to enable the Automated Mode, but want to restrict network access to RPC configuration menus, it is recommended to enable and configure the IP Security Function as described in Section 5.9.3.*

To enable/disable Automated Mode via the Text Interface, access the System Parameters menu (see Section 5.3,) and then use the Automated Mode function in the Scripting Options submenu. To enable/disable the Automated Mode via the Web Browser Interface, place the cursor over the "General Parameters" link; when the flyout menu appears, select "Scripting Options" feature. When Automated Mode is enabled, RPC functions will change as follows:

1. **All Password Security Suppressed:** When a user attempts to access command mode, the password prompt will not be displayed at either the Console Port or the Network Port. Unless specifically restricted by the IP Security Function, all users will be allowed to access both switching and configuration functions, and all commands will be immediately accepted without the requirement to enter a password.
2. **Status Screen Suppressed:** The status screens will not be automatically displayed after commands are successfully executed. Note however, that the /S command can still be invoked to display the status screen as needed.
3. **"Sure?" Prompt Suppressed:** All commands are executed without prompting for user confirmation.
4. **Error Messages Suppressed:** If the **[Enter]** key is pressed without entering a command, the RPC will not respond with the "Invalid Command" message. Note however, that an error message will still be generated if commands are invoked using invalid formats or arguments.

All other status display and configuration commands will still function as normal.

9.4. The SSH/Telnet Connect Function (Web Browser Interface Only)

The SSH/Telnet Connect function allows you to open an SSH Shell Session or Telnet Session without leaving the Web Browser interface. Once you have successfully opened an SSH Shell Session or Telnet Session, you can then use ASCII commands to configure and operate the RPC unit as described in Section 9.2 and Section 17.

9.4.1. Initiating an SSH Shell Session via the Web Browser Interface

To initiate an SSH Shell Session from the RPC Web Browser Interface, proceed as follows:

1. Place the cursor over the "SSH/Telnet Connect" button on the left hand side of the screen. When the flyout menu appears, click on the SSH option.

   Note: *If the RSP displays a message that indicates that your browser does not include the Java plugin, go to the Java website and download the latest version of the Java plugin.*

2. Start Java: Click on the File menu and select "Open Shell Session"

3. The RPC will display a prompt that asks the user to enter a valid username and host name (IP Address.) Key in the username and host name (IP address) using the following format and then click on the "OK" button:

   `username@ip_address`

   Notes:

   - *The username entered must be a valid username that has been previously defined via the RPC User Directory as described in Section 5.5.*
   - *The IP Address (host name) can either be the address to the machine that you are currently communicating with via the Web Browser Interface, or you can enter the IP address for another RPC unit, providing that the username entered is present on the other RPC unit too.*

4. After the username and host name are entered, the RPC will prompt you to enter your password. Key in the password that has been defined for the username entered in step 3 above and then click on the "OK" button.

5. The RPC will display the Circuit Status Screen, followed by the RPC> command prompt. You may now invoke RPC commands as described in Section 9.2 and 17.

6. To terminate the SSH Session, type **`/x`** and press **[Enter]**.

9.4.2. Initiating a Telnet Session via the Web Browser Interface

To initiate a Telnet Session from the RPC Web Browser Interface, proceed as follows:

1. Place the cursor over the "SSH/Telnet Connect" button on the left hand side of the screen. When the flyout menu appears, click on the Telnet option.

   Note: *If the RSP displays a message that indicates that your browser does not include the Java plugin, go to the Java website and download the latest version of the Java plugin.*

2. Log in to the Telnet Session:

   a) The RPC will display the "login" prompt. Key in a valid username that has been previously defined via the RPC User directory and then press **[Enter]**.

   b) The RPC will display the "password" prompt. Key in the valid password for the username entered above and then press **[Enter]**.

   Notes:

   - *The username entered must be a valid username that has been previously defined via the RPC User Directory as described in Section 5.5.*
   - *The IP Address (host name) can either be the address to the machine that you are currently communicating with via the Web Browser Interface, or you can enter the IP address for another RPC unit, providing that the username entered is present on the other RPC unit too.*

3. The RPC will display the Circuit Status Screen, followed by the RPC> command prompt. You may now invoke RPC commands as descrived in Section 9.2 and 17.

4. To terminate the Telnet Session, type **`/x`** and press **[Enter]**.

9.5. Manual Operation

In addition to the command driven functions available via the Web Browser Interface and Text Interface, some RPC functions can also be controlled manually. For a summary of front panel control functions, please refer to Section 2.

9.6. Logging Out of Command Mode

When you have finished communicating with the RPC, it is important to always disconnect using either the "LogOut" link (Web Browser Interface) or the /X command (Text Interface), rather than by simply closing your browser window or communications program. When communicating via a PDA, use the PDA's "Close" function to disconnect and logout.

When you disconnect using the LogOut link or /X command, this ensures that the RPC has completely exited from command mode, and is not waiting for the inactivity timeout period to elapse before allowing additional connections.

10. SSH Encryption

In addition to standard Telnet protocol, the RPC also supports SSH connections, which provide secure, encrypted access via network. In order to communicate with the RPC using SSH protocol, your network node must include an appropriate SSH client.

Note that when the /K (Send SSH Key) command is invoked, the RPC can also provide you with a public SSH key, which can be used to streamline connection to the RPC when using SSH protocol.

Although you can establish an SSH connection to the unit *without* the public key, the public key provides validation for the RPC, and once this key is supplied to the SSH client, the client will no longer display a warning indicating that the RPC is not a recognized user when the client attempts to establish a connection.

The /K command uses the following format:

`/K <k>` [Enter]

Where **`k`** is an argument that determines which type of public key will be displayed, and the **`k`** argument offers the following options:

1. SSH1
2. SSH2 RSA
3. SSH2 DSA

For example, to obtain the public SSH key for an SSH2 RSA client, type **`/K 2`** and then press **[Enter]**. Note that when capturing the SSH key, you can either configure your terminal application to receive the parameter file, or simply copy and paste the resulting SSH key.

Notes:

- *Although the RPC does not support SSH1, the /K 1 command will still return a key for SSH1.*
- *When capturing the SSH key, you can either configure your terminal application to receive the parameter file, or simply copy and paste the resulting key*

11. Syslog Messages

The Syslog feature can create log records of each Alarm Event. As these event records are created, they are sent to a Syslog Daemon, located at an IP address defined via the Network Parameters menu.

11.1. Configuration

If you wish to employ this feature, you must set the real-time clock and calendar via the System Parameters Menu, and define the IP address for the Syslog Daemon via the Network Port Configuration menu.

To configure the Syslog function, please proceed as follows:

1. **Access command mode:** Note that the following configuration menus are only available to accounts that permit Administrator level commands.
2. **System Parameters Menu:** Access the System Parameters Menu as described in Section 5.3, then set the following parameters:
   a) **Set Clock and Calendar:** Set the Real Time Clock and Calendar and/or configure and enable the NTP server feature.
3. **Network Parameters Menu:** Access the Network Parameters Menu as described in Section 5.9, then set the following parameters:
   a) **Syslog IP Address:** Determine the IP address for the device that will run the Syslog Daemon, then use the Network Port Configuration menu to define the IP Address for the Syslog Daemon.

   Note: *The Syslog Address submenu in the Text Interface includes a Ping Test function that can be used to ping the user-selected Syslog IP Address to verify that a valid IP address has been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
4. **Syslog Daemon:** In order to capture messages sent by the RPC, a computer must be running a Syslog Daemon (set to UDP Port 514) at the IP address specified in Step 3 above.

Once the Syslog Address is defined, Syslog messages can be generated whenever one of the alarms discussed in Section 7 is triggered.

12. SNMP Traps

The SNMP Trap function allows the RPC to send Alarm Notification messages to two different SNMP managers, wnenever one of the Alarms discussed in Section 7 is triggered.

Note:

- *The SNMP feature cannot be configured via the SNMP Manager.*
- *SNMP reading ability is limited to the System Group.*
- *The SNMP feature includes the ability to be polled by an SNMP Manager.*
- *Once SNMP Trap Parameters have been defined, SNMP Traps will be sent each time an Alarm is triggered. For more information on Alarm Configuration, please refer to Section 7.*

12.1. Configuration

To configure the SNMP Trap function, proceed as follows:

1. Access command mode using an account that permits Administrator level commands.
2. **SNMP Trap Parameters:** Access the SNMP Trap Parameters Menu as described in Section 5.9.7. Set the following:
   a) **SNMP Managers 1 and 2:** The address(es) that will receive SNMP Traps that are generated by one of the Alarms discussed in Section 7. Consult your network administrator to determine the IP address(es) for the SNMP Manager(s), then use the Network Parameters menu to set the IP address for each SNMP Manager. Note that it is not necessary to define both SNMP Managers.

Notes:

- *To enable the SNMP Trap feature, you must define at least one SNMP Manager. SNMP Traps are automatically enabled when at least one SNMP Manager has been defined.*
- *The SNMP Trap submenu in the Text Interface includes a Ping Test function that can be used to ping the user-selected SNMP Managers to verify that a valid IP address has been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*

   b) **Trap Community:** Consult your network administrator, and then use the Network Parameters menus to set the Trap Community.

Once SNMP Trap Parameters have been defined, the RPC will send an SNMP Trap each time an alarm is triggered.

13. Operation via SNMP

If SNMP Access Parameters have been defined as described in Section 5.9.6, then you will be able to manage user accounts, control power and reboot switching and display unit status via SNMP. This section describes SNMP communication with the RPC unit, and lists some common commands that can be employed to manage users, control switching and reboot actions and display unit status.

Note: *SNMP Commands are not available when the IPS mode is active.*

13.1. RPC SNMP Agent

The RPC's SNMP Agent supports various configuration, control, status and event notification capabilities. Managed objects are described in WTI-MPC-VMR-MIB.txt, which can be found in the user's guide archive on the WTI web site at: (http://www.wti.com/manuals.htm).

The WTI-MPC-VMR-MIB.txt document can be compiled for use with your SNMP client.

13.2. SNMPv3 Authentication and Encryption

The major limitations of SNMPv2 were the failure to include proper username/password login credentials (v2 only used a password type of login, i.e., community name) and the exclusion of encryption for data moving over the internet. SNMPv3 addresses both of these shortcomings.

For SNMPv3, the RPC supports two forms of Authentication/Privacy: Auth/noPriv which requires a username/password, but does not encrypt data going over the internet and Auth/Priv which requires a username/password AND encrypts the data going over the internet using DES (AES is not supported at this time). For the Password protocol, the RPC supports either MD5 or SHA1.

13.3. Configuration via SNMP

RPC User accounts can be viewed, created, modified, and deleted via SNMP. User accounts are arranged in a table of 128 rows, and indexed 1-128. User account parameters, as seen through the SNMP, are summarized below.

- **`userTable::userName`** – 32 character username
- **`userTable::userPasswd`** – 16 character password
- **`userTable::userAccessLevel`** – Account access level.
  `0` – View Access
  `1` – User Access
  `2` – Superuser Access
  `3` – Administrator Access
- **`userTable::userLocalAccess`** – A string of 8characters, with one character for each of the 8 possible circuits on the RPC unit. A '`0`' indicates that the account **does not** have access to the circuit, and a '`1`' indicates that the user *does* have access to the circuit.
- **`userTable::userGroupAccess`** – A string of 54 characters, with one character for each of the 54 possible circuit groups in the system. '`0`' indicates that the account **cannot** access the group, and '`1`' indicates that the user *can* access the group.
- **`userTable::userSerialAccess`** – Access to the serial interface
  `0` – No access
  `1` – Access
- **`userTable::userTelnetSshAccess`** – Access to the Telnet/SSH interface.
  `0` – No access
  `1` - Access
- **`userTable::userOutboundTelSshAccess`** – Access to Outbound Telnet/SSH
  `0` – No access
  `1` - Access
- **`userTable::userWebAccess`** – Access to the Web interface.
  `0` – No access
  `1` - Access
- **`userTable::userCallbackNum`** – 32 character callback number for account.
- **`userTable::userSubmit`** – Set to `1` to submit changes.

13.3.1. Viewing Users

To view users, issue a GET request on any of the user parameters for the index corresponding to the desired user.

13.3.2. Adding Users

For an empty index, issue a SET request on the desired parameters. Minimum requirement is a username and password to create a user, all other parameters will be set to defaults if not specified. To create the user, issue a SET request on the userSubmit object.

13.3.3. Modifying Users

For the index corresponding to the user you wish to modify, issue a SET request on the desired parameters to be modified. Once complete, issue a SET request on the userSubmit object.

13.3.4. Deleting Users

For the index corresponding to the user you wish to delete, issue a SET request on the username with a blank string. Once complete, issue a SET request on the userSubmit object.

13.4. Circuit Control via SNMP

13.4.1. Circuit Status/Control

ON, OFF, BOOT, and DEFAULT commands can be issued for circuits via SNMP. Circuits are arranged in a table of N rows, where N is the number of circuits in the system. Circuit parameters are described below.

- **plugTable::plugID** – String indicating the circuit's ID.
- **plugTable::plugName** – String indicating the circuit's user-defined name.
- **plugTable::plugStatus** – Current state of the circuit.
  - **0** – Circuit is OFF
  - **1** – Circuit is ON
- **plugTable::plugAction** – Action to be taken on circuit.
  - **1** – Mark to turn ON (does not execute)
  - **2** – Mark to turn OFF (does not execute)
  - **3** – Mark to BOOT (does not execute)
  - 4 – Mark to DEFAULT (does not execute)
  - 5 – Mark to turn ON and execute circuit actions
  - 6 - Mark to turn OFF and execute circuit actions
  - 7 - Mark to BOOT and execute circuit actions
  - 8 - Mark to DEFAULT and execute circuit actions

Set **plugTable::plugAction** to desired action, as specified by values 1-4 above, for each circuit index the action is to be applied to. For the last circuit you wish to set before executing the commands, use values 5-8 instead, which will invoke the requested commands all at once.

13.4.2. Circuit Group Status/Control

ON, OFF, BOOT, and DEFAULT commands can be issued for circuit groups via SNMP. Circuit groups are arranged in a table of 54 rows, one row for each circuit group in the system. Circuit Group parameters are described below.

- **plugGroupTable::plugGroupName** – String indicating the circuit groups name.
- **plugGroupTable::plugGroupAction** – Action to be taken on circuit group
  - **1** – Mark to turn ON (does not execute)
  - **2** – Mark to turn OFF (does not execute)
  - **3** – Mark to BOOT (does not execute)
  - **4** – Mark to DEFAULT (does not execute)
  - **5** – Mark to turn ON and execute circuit group actions
  - **6** – Mark to turn OFF and execute circuit group actions
  - **7** – Mark to BOOT and execute circuit group actions
  - **8** – Mark to DEFAULT and execute circuit group actions

Set **plugGroupTable::plugGroupAction** to desired action, as specified by values 1-4 above, for each circuit group index the action is to be applied to. For the last circuit group you wish to set before executing the commands, use values 5-8 instead, which will invoke the requested commands all at once.

13.5. Viewing RPC Status via SNMP

Status of various components of the RPC can be retrieved via SNMP. Circuit Status, and Environmental Status are currently supported.

13.5.1. System Status - Ethernet Port Mac Addresses

The Mac Address for the Ethernet Port can be displayed using the command below:

- **`environmentUnitTable::environmentMacEth0`** The Mac Address for Ethernet Port 0.

13.5.2. Circuit Status

The status of each circuit in the system can be retrieved using the command below.

- **`plugTable::plugStatus`** – The status of the circuit.
  `0` – Circuit is OFF
  `1` – Circuit is ON
- **`plugTable::plugName`** - String indicating the circuit's user-defined name.

13.5.3. Unit Environment Status

The temperature reading can be retrieved from the RPC unit.

- **`environmentUnitTable::environmentUnitName`** – The unit (LOCAL.)
- **`environmentUnitTable::environmentUnitTemperature`** – The temperature of the given unit.

13.5.4. Alarm Status

The status of the VMR/NPS unit's alarm functions can be retrieved and displayed using the following commands:

Notes:

- *When an alarm status command returns a zero (0), this indicates that the alarm is inactive.*
- *When an alarm status command returns a one (1), this indicates that the alarm is active (triggered.)*

- **`alarmTables::alarmOverTemperatureInitial`** - Displays the status of the Over Temperature (Initial) Alarm.
- **`alarmTables::alarmOverTemperatureCritical`** - Displays the status of the Over Temperature (Critical) Alarm.
- **`alarmTables::alarmCircuitBreakerOpen`** - Displays the status of the Circuit Breaker Open Alarm.
- **`alarmTables::alarmPingNoAnswer`** - Displays the status of the Ping-No-Answer Alarm.
- **`alarmTables::alarmInvalidAccessLockout`** - Displays the status of the Serial Port Invalid Access Lockout Alarm.
- **`alarmTables::alarmPowerCycle`** - Displays the status of the Power Cycle Alarm.
- **`alarmTables::alarmLostOptoVoltage`** - (Dual Power Inlet Units Only) Displays the status of the Lost Voltage Alarm.
- **`alarmTables::alarmNoDialtone`** - Displays the status of the No Dialtone Alarm.
- **`alarmTables::alarmEmergencyShutoff`** - Displays the status of the Emergency Shut Off feature. For more information regarding the Emergency Shut Off feature, please contact WTI Tech Support at service@wti.com.

13.6. Sending Traps via SNMP

Traps that report various unit conditions can be sent to an SNMP Management Station from the RPC. The following traps are currently supported.

- **`WarmStart`** Trap – Trap indicating a warm start
- **`ColdStart`** Trap – Trap indicating a cold start
- **`Test`** Trap – Test trap invoked by user via the Text Interface (CLI.)

The RPC can send an SNMP trap to notify you when any of the available alarm functions have been triggered. In all cases except the Power Cycle Alarm, there will be one trap sent when the alarm is triggered, and a second trap sent when the alarm is cleared. For more information on alarm functions, please refer to Section 7.

- **`Alarm`** Trap – Trap indicating an alarm condition. A trap with a unique enterprise OID is defined for every possible alarm in the system, under which several specific trap-types are defined to indicate the setting or clearing of that particular alarm condition.
- **`overTemperatureInitialSetTrap`** - Indicates that the Over Temperature (Initial) Alarm has been triggered. The trap will also include a numerical value that indicates the current unit temperature.
- **`overTemperatureInitialClearTrap`** - Indicates that the Over Temperature (Initial) Alarm has been cleared.
- **`overTemperatureCriticalSetTrap`** - Indicates that the Over Temperature (Critical) Alarm has been triggered. The trap will also include a numerical value that indicates the current unit temperature.
- **`overTemperatureCriticalClearTrap`** - Indicates that the Over Temperature (Critical) Alarm has been cleared.
- **`pingNoAnswerSetTrap`** - Indicates that the Ping No Answer Alarm has been triggered. The trap will also include a numerical value that indicates the IP address of the device that failed to respond to the ping command.
- **`pingNoAnswerClearTrap`** - Indicates that the Ping No Answer Alarm has been cleared.
- **`lockoutSetTrap`** - Indicates that the Invalid Access Lockout Alarm has been triggered. The trap will also include a numerical value that indicates the number of the serial port where the lockout occurred.
- **`lockoutClearTrap`** - Indicates that the Invalid Access Lockout Alarm has been cleared.
- **`powercycleSetTrap`** - Indicates that the Power Cycle Alarm has been triggered (Note that there is no corresponding Clear Trap for the Power Cycle Alarm.)
- **`lostCommSetTrap`** - Indicates that the Lost Communication Alarm has been triggered.
- **`lostOptoVoltageSetTrap`** - Indicates that the Lost Voltage Alarm has been triggered at a unit that includes opto sensors.
- **`lostOptoVoltageClearTrap`** - Indicates that the Lost Voltage Alarm has been cleared at a unit that includes opto sensors.

- **`noDialtoneSetTrap`** - Indicates that the No Dialtone Alarm has been triggered.
- **`noDialtoneClearTrap`** - Indicates that the No Dialtone Alarm has been cleared.
- **`emergencyShutoffSetTrap`** - Indicates that an emergency shut off has been implemented. For more information regarding the Emergency Shut Off feature, please contact WTI Tech Support at service@wti.com.
- **`emergencyShutoffClearTrap`** - Indicates that an emergency shut off has been cleared. For more information regarding the Emergency Shut Off feature, please contact WTI Tech Support at service@wti.com.

14. Setting Up SSL Encryption

This section describes the procedure for setting up a secure connection via an https web connection to the RPC.

> **Note:** *SSL parameters cannot be defined via the Web Browser Interface. In order to set up SSL encryption, you must contact the RPC via the Text Interface.*

There are two different types of https security certificates: "Self Signed" certificates and "Signed" certificates.

Self Signed certificates can be created by the RPC, without the need to go to an outside service, and there is no need to set up your domain name server to recognize the RPC. The principal disadvantage of Self Signed certificates, is that when you access the RPC command mode via the Web Browser Interface, the browser will display a message which warns that the connection might be unsafe. Note however, that even though this message is displayed, communication will still be encrypted, and the message is merely a warning that the RPC is not recognized and that you may not be connecting to the site that you intended.

Signed certificates must be created via an outside security service (e.g., VeriSign®, Thawte™, etc.) and then uploaded to the RPC unit to verify the user's identity. In order to use Signed certificates, you must contact an appropriate security service and set up your domain name server to recognize the name that you will assign to the RPC unit (e.g., service.wti.com.) Once a signed certificate has been created and uploaded to the RPC, you will then be able to access command mode without seeing the warning message that is normally displayed for Self Signed certificate access.

```
WEB ACCESS: [eth0] IPv4

HTTP:
1.  Enable: On
2.  Port:   80

HTTPS:
3.  Enable: Off
4.  Port:   443

SSL Certificates:
5.  Common Name:
6.  State or Province:
7.  Locality:
8.  Country:
9.  Email Address:
10. Organization Name:
11. Organizational Unit:              15. Export Server Private Key:
12. Create CSR:                       16. Import Server Private Key:
13. View CSR:                         17. Harden Web Security: Medium
14. Import CRT:                       18. TLS Mode: TLSv1

Enter: #<CR> to change,
       <ESC> to return to previous menu ...
```

Figure 14.1: Web Access Parameters (Text Interface Only)

14.1. Creating a Self Signed Certificate

To create a Self Signed certificate, access the Text interface via Telnet or SSH, using a password that permits access to Administrator level commands and then proceed as follows:

1. Type **/N** and press **[Enter]** to display the Network Parameters menu.
2. At the Network Parameters menu, type **23** and press **[Enter]** to display the Web Access menu (Figure 14.1.) Type **3** and press **[Enter]** and then follow the instructions in the resulting submenu to enable HTTPS access.
3. Next, use the Web Access menu to define the following parameters.

   Note: *When configuring the RPC, make certain to define all of the following parameters. Although most SSL applications require only the Common Name, in the case of the RPC all of the following parameters are mandatory.*

   - **5. Common Name:** A domain name, that will be used to identify the RPC unit. If you will use a Self Signed certificate, then this name can be any name that you choose, and there is no need to set up your domain name server to recognize this name. However, if you will use a Signed certificate, then your domain name server must be set up to recognize this name (e.g., service.wti.com.)
   - **6. State or Province:** The name of the state or province where the RPC unit will be located (e.g., California.)
   - **7. Locality:** The city or town where the RPC unit will be located (e.g., Irvine.)
   - **8. Country:** The two character country code for the nation where the RPC will be located (e.g., US.)
   - **9. Email Address:** An email address, that can be used to contact the person responsible for the RPC (e.g., jsmith@yourcompany.com.)
   - **10. Organizational Name:** The name of your company or organization (e.g., Western Telematic.)
   - **11. Organizational Unit:** The name of your department or division; if necessary, any random text can be entered in this field (e.g., tech support.)

4. After you have defined parameters 5 through 11, type `12` and press **[Enter]** (Create CSR) to create a Certificate Signing Request. By default, this will overwrite any existing certificate, and create a new Self Signed certificate.

   a) The RPC will prompt you to create a password. Key in the desired password (up to 16 characters) and then press **[Enter]**. When the RPC prompts you to verify the password, key it again and then press **[Enter]** once. After a brief pause, the RPC will return to the Web Access Menu, indicating that the CSR has been successfully created.

   b) When the Web Access Menu is re-displayed, press **[Esc]** several times until you exit from the Network Parameters menu and the "Saving Configuration" message is displayed.

5. After the new configuration has been saved, test the Self Signed certificate by accessing the RPC via the Web Interface, using an HTTPS connection.

   a) Before the connection is established, the RPC should display the warning message described previously. This indicates that the Self Signed certificate has been successfully created and saved.

   b) Click on the "Yes" button to proceed. The RPC will prompt you to enter a user name and password. After keying in your password, the main menu should be displayed, indicating that you have successfully accessed command mode.

14.2. Creating a Signed Certificate

To create a Signed certificate, and eliminate the warning message, first set up your domain name server to recognize the Common Name (item 5) that you will assign to the unit. Next, complete steps one through five as described in Section 14.1 and then proceed as follows:

1. **Capture the Newly Created Certificate:** Type `13` and press **[Enter]** (View CSR). The RPC will prompt you to configure your communications (Telnet) program to receive the certificate. Set up your communications program to receive a binary file, and then press **[Enter]** to capture the file and save it. This is the Code Signing Request that you will send to the outside security service (e.g., VeriSign, Thawte, etc.) in order to have them sign and activate the certificate.

2. **Obtain the Signed Certificate:** Send the captured certificate to the outside security service. Refer to the security service's web page for further instructions.

3. **Upload the Signed Certificate to the RPC:** After the "signed" certificate is returned from the security service, return to the Web Access menu.

   a) Access the RPC command mode via the Text Interface using an account that permits Administrator level commands as described previously, then type **/N** and press **[Enter]** to display the Network Parameters menu, and then type **23** and press **[Enter]** to display the Web Access menu.

   b) From the Web Access menu, type **14** and press **[Enter]** (Import CRT) to begin the upload process. At the CRT Server Key submenu, type **1** and press **[Enter]** to choose "Upload Server Key."

   c) Use your communications program to send the binary format Signed Certificate to the RPC unit. When the upload is complete, press **[Escape]** to exit from the CRT Server Key submenu.

   d) After you exit from the CRT Server Key submenu, press [Escape] several times until you have exited from the Network Parameters menu and the "Saving Configuration" message is displayed.

4. After the configuration has been saved, test the signed certificate by accessing the RPC via the Web Browser Interface, using an HTTPS connection. For example, if the common name has been defined as "service.companyname111.com", then you would enter "**https://service.companyname111.com**" in your web browser's address field. If the Signed Certificate has been properly created and uploaded, the warning message should no longer be displayed.

14.3. Downloading the Server Private Key

When configuring the RPC's SSL encryption feature (or setting up other security/ authentication features), it is recommended to download and save the Server Private Key. To download the Server Private Key, access the Text interface via Telnet or SSH, using a password that permits access to Administrator level commands and then proceed as follows:

1. Type **/N** and press **[Enter]** to display the Network Parameters menu.

2. At the Network Parameters menu, type **23** and press **[Enter]** to display the Web Access menu (Figure 14.1.)

   a) To download the Server Private Key from the RPC unit, make certain that SSL parameters have been defined as described in Section 14.1, then type **15** and press **[Enter]** and store the resulting key on your hard drive.

   b) To upload a previously saved Server Private Key to the RPC unit, make certain that SSL parameters have been defined as described in Section 14.1, then type **16** and press **[Enter]** and follow the instructions in the resulting submenu.

14.4. TLS Mode

The TLS Mode parameter in the Web Access menu (Text Interface Only) allows the TLS Mode to be set to either TLSv1 or TLSv1.1. Although TLSv1.1 provides better security, the default settings of most browsers do not support TLSv1.1. The default setting for this parameter is TLSv1.

15. Saving and Restoring Configuration Parameters

Once the RPC has been properly configured, parameters can be downloaded and saved as an ASCII text file. Later, if the configuration is accidentally altered, the saved parameters can be uploaded to automatically reconfigure the unit without the need to manually assign each parameter.

Saved parameters can also be uploaded to other identical RPC units, allowing rapid set-up when several identical units will be configured with the same parameters.

The "Save Parameters" procedure can be performed from any terminal emulation program (e.g. HyperTerminal™, TeraTerm©, etc.,) that allows downloading of ASCII files.

> **Note:** *Configuration parameters can be downloaded and saved via either the Web Browser Interface or Text Interface. Saved configuration parameters can only be uploaded to the unit via the Text Interface.*

15.1. Sending Parameters to a File

15.1.1. Downloading & Saving Parameters via Text Interface

1. Start your terminal emulation program and access the Text Interface command mode using an account that permits Administrator level commands.
2. When the command prompt appears, type `/u` and press **[Enter]**. The RPC will prompt you to configure your terminal emulation program to receive an ASCII download.
   a) Set your terminal emulation program to receive an ASCII download, and the specify a name for a file that will receive the saved parameters (e.g. RPC.PAR).
   b) Disable the Line Wrap function for your terminal emulation program. This will prevent command lines from being broken in two during transmission.
3. When the terminal emulation program is ready to receive the file, return to the RPC's Save Parameter File menu, and press **[Enter]** to proceed. RPC parameters will be saved on your hard drive in the file specified in Step 2 above.
4. The RPC will send a series of ASCII command lines which specify currently selected parameters. When the download is complete, press **[Enter]** to return to the command prompt.

15.1.2. Downloading & Saving Parameters via Web Browser Interface

The Web Browser Interface also includes a download function that can be used to save RPC parameters to an XML format file on your PC or laptop. To save parameters via the Web Browser Interface, proceed as follows:

Notes:

- *Although RPC parameters can be saved to a file via either the Text Interface or Web Browser Interface, saved parameters can only be restored via the Text Interface. The Restore Parameters function is not available via the Web Browser Interface.*
- *This procedure may differ slightly, depending on the operating system and browser used. In some cases, your system may perform a security scan before proceding with the download.*

1. Access the Web Browser Interface command mode using an account that permits Administrator level commands.
2. When the Web Browser Interface appears, click on the "Download Unit Configuration" button on the left hand side of the screen.
3. After a brief pause, your browser may display a prompt asking if you want to open or save the downloaded file. At this point, you can either select the "Save" option to save the parameters file to the download folder on your PC, or select "Save As" to pick a different location and/or filename for the saved parameters file.

15.2. Restoring Saved Parameters

This section describes the procedure for using your terminal emulation program to send saved parameters to the RPC.

Note: *The Restore Parameters feature is only available via the Text Interface.*

1. Start your terminal emulation program and access the RPC's Text Interface command mode using an account that permits Administrator level commands.
2. Configure your terminal emulation program to upload an ASCII text file.
3. Upload the ASCII text file with the saved RPC parameters. If necessary, key in the file name and directory path.
4. Your terminal emulation program will send the ASCII text file to the RPC. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

   Note: *If the RPC detects an error in the file, it will respond with the "Invalid Parameter" message. If an error message is received, carefully check the contents of the parameters file, correct the problem, and then repeat the Upload procedure.*

5. If the parameter upload is successful, the RPC will send a confirmation message, and then return to the command prompt. Type `/s` and press **[Enter]**, the Status Screen will be displayed. Check the Status Screen to make certain the unit has been configured with the saved parameters.

15.3. Restoring Previously Saved Parameters

If you make a mistake while configuring the RPC unit, and wish to return to the previously saved parameters, the Text Interface's "Reboot System" command (`/I`) offers the option to reinitialize the RPC unit using previously backed up parameters. This allows you to reset the unit to previously saved parameters, even after you have changed parameters and saved them.

Notes:

- *The RPC will automatically backup saved parameters once a day, shortly after Midnight. This configuration backup file will contain only the most recently saved RPC parameters, and will be overwritten by the next night's daily backup.*
- *When the /I command is invoked, a submenu will be displayed which offers several Reboot options. Options 5 is used to restore the configuration backup file. The date shown next to options 5 indicates the date that you last changed and saved unit parameters.*
- *If the daily automatic configuration backup has been triggered since the configuration error was made, and the previously saved configuration has been overwritten by newer, incorrect parameters, then this function will not be able to restore the previously saved (correct) parameters.*

To restore the previously saved configuration, proceed as follows:

1. Access command mode via the Text Interface, using a username/password that permits access to Administrator level commands (see Section 5.1.1.)
2. At the RPC command prompt, type `/I` and press **[Enter]**. The RPC will display a submenu that offers several different reboot options.
3. At the submenu, you may choose Item 5 (Reboot & Restore Last Known Working Configuration.) Type `5` and press **[Enter]**.

   Note: *When invoking the /I command to restore configuration parameters, Item 5 is recommended.*
4. The RPC will reboot and previously saved parameters will be restored.

16. Upgrading RPC Firmware

When new, improved versions of the RPC firmware become available, either the Firmware Upgrade Utility (recommended) or the "Upgrade Firmware" function (Text Interface only) can be used to update the unit. The following Section describes the procedure for updating the RPC unit using the Firmware Upgrade Utility or the Upgrade Firmware function.

16.1. WMU Enterprise Management Software (Recommended)

The preferred method for updating RPC units is via the WMU Enterprise Management Software that is included with the unit. The WMU software allows you to manage firmware updates for multiple WTI units from a single interface. For a description of the process for managing firmware updates via the WMU, please refer to the WMU user's guide, which can be downloaded from the WTI User's Guide Archive at:

http://www.wti.com/t-product-manuals.aspx

Note that in order to use the WMU software, the firmware version for the RPC must be at least v1.48 or higher. When upgrading older RPC units that feature pre v1.48 firmware, it is recommended to use the WTI Firmware Upgrade Utility. A zip file that contains the installation files and other documentation for the WTI Firmware Upgrade Utility can be downloaded from WTI's FTP server, located at:

ftp://wtiftp.wti.com/pub/TechSupport/Firmware/Upgrade_Utility/

Please refer to the documentation included in the zip file for further instructions.

16.2. The Upgrade Firmware Function (Alternate Method)

The Upgrade Firmware function provides an alternative method for updating the RPC firmware. Updates can be uploaded via FTP or SFTP protocols.

Notes:

- *The FTP/SFTP servers can only be started via the Text Interface.*
- *All other ports will remain active during the firmware upgrade procedure.*
- *If the upgrade includes new parameters or features not included in the previous firmware version, these new parameters will be set to their default values.*
- *The upgrade procedure will require approximately 15 minutes.*

1. Obtain the update file. Firmware modifications can either be mailed to the customer, or downloaded from WTI. Place the upgrade CDR in your disk drive or copy the file to your hard drive.
2. Access Text Interface command mode via Serial Port, Telnet or SSH client session, using a username/password and port that permit Administrator level commands.

3. When the command prompt appears, type **/UF** and then press **[Enter]**. The RPC will display a screen which offers the following options:

   a) **Start FTP/SFTP Servers Only (Do NOT default parameters):** To proceed with the upgrade, while retaining user-defined parameters, type **1** and press **[Enter]**. All existing parameter settings will be restored when the upgrade is complete.

   b) **Start FTP/SFTP Servers & Default (Keep IP parameters & SSH Keys):** To proceed with the upgrade and default all user-defined parameters except for the IP Parameters and SSH Keys, type **2** and press **[Enter]**. When the upgrade is complete, all parameter settings except the IP Parameters and SSH Keys, will be reset to factory default values.

   c) **Start FTP/SFTP Servers & Default (Default ALL parameters):** To proceed with the upgrade, and reset parameters to default settings, type **3** and press **[Enter]**. When the upgrade is complete, all parameters will be set to default values.

   d) **Start FTP/SFTP Servers for Slip Stream Upgrade:** This option will upgrade only the WTI Management Utility, without updating the RPC's operating firmware. To update the WTI Management Utility only, type **4** and press **[Enter]**.

   Note that after any of the above options is selected, the RPC will start the receiving servers and wait for an FTP/SFTP client to make a connection and upload a valid firmware binary image.

4. To proceed with the upgrade, select the desired option. The RPC will display a message that indicates that the unit is waiting for data. Leave the current Telnet/SSH client session connected at this time.

5. Open your FTP/SFTP application and (if you have not already done so,) login to the RPC unit, using a username and password that permit access to Administrator level commands.

6. Transfer the md5 format upgrade file to the RPC.

7. After the file transfer is complete, the RPC will install the upgrade file and then reboot itself and break all port connections. Note that it will take approximately 10 minutes to complete the installation process. The unit will remain accessible until it reboots.

   a) Some FTP/SFTP applications may not automatically close when the file transfer is complete. If this is the case, you may close your FTP/SFTP client manually after it indicates that the file has been successfully transferred.

   b) When the upgrade process is complete, the RPC will send a message to all currently connected network sessions, indicating that the RPC is going down for a reboot.

   Note: *Do not power down the RPC unit while it is in the process of installing the upgrade file. This can damage the unit's operating system.*

8. If you have accessed the RPC via the Network Port, in order to start the FTP/SFTP servers, the RPC will break the network connection when the system is reinitialized.

   - If you initially selected "Start FTP/SFTP Servers and Save Parameters", you may then reestablish a connection with the RPC using your former IP address.
   - If you initially selected "Start FTP/SFTP Servers and Default Parameters", you must then login using the RPC's default IP address (Default = 192.168.168.168) or access command mode via Serial Port 1 or 2 or via Modem.

When firmware upgrades are available, WTI will provide the necessary files. At that time, an updated Users Guide or addendum will also be available.

17. Command Reference Guide

17.1. Command Conventions

Most commands described in this section conform to the following conventions:

- **Text Interface:** Commands discussed in this section, can only be invoked via the Text Interface. These commands *cannot* be invoked via the Web Browser Interface.
- **Slash Character:** Most RPC Text Interface commands begin with the Slash Character (**/**).
- **Apply Command to All Circuits:** When an asterisk is entered as the argument of the **/ON** (Switch Circuits On), **/OFF** (Switch Circuits Off) or **/BOOT** (Reboot Circuits) commands, the command will be applied to all circuits. For example, to reboot all allowed circuits, type **/BOOT * [Enter]**.
- **Command Queues:** If a switching or reboot command is directed to a circuit that is already being switched or rebooted by a previous command, then the new command will be placed into a queue until the circuit is ready to receive additional commands.
- **"Busy" Circuits:** If the "Status" column in the Circuit Status Screen includes an asterisk, this means that the circuit is currently busy, and is in the process of completing a previously issued command. If a new command is issued to a busy circuit, then the new command will placed into a queue to be executed later, when the circuit is ready to receive additional commands.
- **Circuit Name Wild Card:** It is not always necessary to enter the entire circuit name. Circuit names can be abbreviated in command lines by entering the first character(s) of the name followed by an asterisk (*****). For example, a circuit named "SERVER" can be specified as "**S***". Note however, that this command would also be applied to any other circuit name that begins with an "S".
- **Suppress Command Confirmation Prompt:** When the **/ON** (Switch Circuit On), **/OFF** (Switch Circuit Off), **/BOOT** (Reboot Circuit) or **/DPL** (Default All Circuits) commands are invoked, the "**,Y**" option can be included to override the Command Confirmation ("Sure?") prompt. For example, to reboot Circuit A4 without displaying the Sure prompt, type **/BOOT A4,Y [Enter]**.
- **Enter Key:** Most commands are invoked by pressing **[Enter]**.
- **Configuration Menus:** To exit from a configuration menu, press **[Esc]**.

17.2. Command Summary

Function	Command Syntax	Command Access Level			
		Admin.	SuperUser	User	ViewOnly
Display					
Circuit Status	**/S [s] [Enter]**	X❶	X❶	X❶	X❶
Port Diagnostics	**/SD [Enter]**	X❶	X❶	X❶	X❶
Circuit Group Status	**/SG [Enter]**	X❷	X❷	X❷	X❷
Network Status	**/SN [Enter]**	X	X	X	X
Network Configuration Summary	**/RN [Enter]**	X	X	X	X
IP Alias Status	**/SA [Enter]**	X	X	X❶	X❶
Alarm Status	**/AS [Enter]**	X			
Help Menu	**/H [Enter]**	X❸	X❸	X❸	X❸
Log Functions	**/L [Enter]**	X	X		
Site ID / Unit Information	**/J** [*] **[Enter]❹**	X	X	X	X
Control					
Exit Command Mode	**/X [Enter]**	X	X	X	X
Boot Circuit *n*	**/BOOT <s>[,Y] [Enter]❺**	X	X	X	
Turn Circuit *n* On	**/ON <s>[,Y] [Enter]❺**	X	X	X	
Turn Circuit *n* Off	**/OFF <s>[,Y] [Enter]❺**	X	X	X	
Default All Circuits	**/DPL[,Y] [Enter]❺**	X	X	X	
Connect to Port	**/C [n] [Enter]**	X	X	X	
Disconnect from Port	**/D [n] [Enter]**	X	X	X	
Send Parameter File	**/U [Enter]**	X			
Send SSH Keys	**/K <k> [Enter]**	X			
Unlock Invalid Access	**/UL [Enter]**	X			
Outbound Telnet	**/TELNET <ip> [port] [raw] [Enter]**	X❻	X❻	X❻	
Outbound SSH	**/SSH <ip> -l <username> [Enter]**	X❻	X❻		
Configuration					
System Parameters	**/F [Enter]**	X	❼		
Console Port Parameters	**/P [n] [Enter]**	X	❼		
Circuit Parameters	**/PL [Enter]**	X	❼		
Circuit Group Parameters	**/G [Enter]**	X	❼		
Network Configuration - IPv4	**/N [Enter]**	X	❼		
Network Configuration - IPv6	**/N6 [Enter]**	X	❼		
Reboot Options	**/RB [Enter]**	X	❼		
Alarm Configuration	**/AC [Enter]**	X	❼		
Reboot System	**/I [Enter]**	X	❼		
Upgrade Firmware	**/UF [Enter]**	X			
Test Network Configuration	**/TEST [Enter]**	X			

❶ In Administrator Mode and SuperUser Mode, all RPC circuits are displayed. In User Mode and ViewOnly Mode, the Circuit Status Screen will only include the circuits that are allowed by your account.

❷ In Administrator Mode, all Circuit Groups are displayed. In SuperUser Mode, User Mode and ViewOnly Mode, the Circuit Group Status Screen will only include the Circuit Groups that are allowed by your account.

❸ In Administrator Mode, the Help Menus will list all RPC commands. In the SuperUser Mode, User Mode and ViewOnly Mode, the Help Menus will only list the commands that are allowed by the access level.

❹ If the optional asterisk (*****) argument is included in the command line, this command will also show model numbers, software versions and other information for the RPC unit.

❺ The "**,Y**" argument can be included in the command line to suppress the command confirmation prompt.

❻ In order to invoke this command, Outbound Telnet/SSH and Outbound SErvice Access must be enabled for your account.

❼ In SuperUser Mode, configuration menus can be displayed, but parameters cannot be changed.

17.3. Command Set

This Section provides information on all Text Interface commands, sorted by functionality

17.3.1. Display Commands

/S Display Circuit Status Screen

Displays the Circuit Status Screen, which lists the current On/Off state, plus the circuit number, circuit name, Boot/Sequence Delay value and Default On/Off value for each circuit. For more information, please refer to Section 8.3.

Note that the /S command line can also include arguments that display On/Off status for an individual circuit, two or more specific circuits, or a range of several circuits:

- `/S` Displays configuration details and On/Off status for all switched circuits.
- `/S s` Displays On/Off status for an individual circuit, where *s* is the name or number of the desired circuit.
- `/S s+s` Displays status information for two or more specific circuits, where *s* is the number or name of each desired circuit. A plus sign (+) is entered between each circuit number or name.
- `/S s:s` Displays status information for a range of circuits, where *s* is the number or name of the circuit at the beginning and end of the range of desired circuits. A colon (:) is entered between the two circuit numbers or names that mark the beginning of the range and the end of the range.

Notes:

- *In Administrator Mode and SuperUser Mode, all circuits are displayed. In User Mode and ViewOnly Mode, the Circuit Status Screen will only include the circuits allowed by your account.*
- *The RPC will return a "0" to indicate that the circuit is Off, or a "1" to indicate that the circuit is On.*

Availability: Administrator, SuperUser, User, ViewOnly
Format: `/S` **[Enter]**

/SD Display Port Diagnostics

Provides detailed information regarding the status of each port. When this command is issued by a User level or View Only level account, the resulting screen will only display parameters for the ports allowed by the account. For more information, please refer to Section 8.5.

Availability: Administrator, SuperUser, User, ViewOnly
Format: `/SD` **[Enter]**
Response: Displays Port Diagnostics Screen.

/SG Display Circuit Group Status Screen

Displays the Circuit Group Status Screen, which lists the available Circuit Groups, the numbers of the circuits included in each Circuit Group, the current On/Off state, the user-defined Boot/Sequence Delay value, and the Default On/Off value for each circuit. For more information, please refer to Section 8.4.

> **Note:** *In Administrator Mode all user defined Circuit Groups are displayed. In SuperUser Mode, User Mode and ViewOnly Mode, the Circuit Group Status Screen will only include the Circuit Groups allowed by your account.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: `/SG` **[Enter]**

/SN Display Network Status

Displays the Network Status Screen, which lists active network connections to the RPC's Network Port. For more information, please refer to Section 8.2.

Availability: Administrator, SuperUser, User, ViewOnly

Format: `/SN` **[Enter]**

/RN Network Configuration Summary

Displays a screen that lists currently selected communication settings, LDAP status, RADIUS status, Email Messaging status, NTP status and PPP status.

Availability: Administrator, SuperUser, User ViewOnly

Format: `/RN` **[Enter]**

/H Help

Displays a Help Screen, which lists all available Text Interface commands along with a brief description of each command.

> **Note:** *In the Administrator Mode, the Help Screen will list the entire RPC Text Interface command set. In SuperUser Mode, User Mode and ViewOnly Mode, the Help Screen will only list the commands that are allowed by the account's access level.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: `/H` **[Enter]**

/L Log Functions

Provides access to a menu which allows you to display the Audit Log, Alarm Log and Temperature Log. For more information on Log Functions, please refer to Section 5.3.3.

Availability: Administrator, SuperUser

Format: **`/L`** **[Enter]**

/AS Alarm Status Screen

Lists all available user-defined alarms and indicates whether or not each alarm has been triggered as described in Section 8.7. The resulting screen will display "Yes" (or 1) for alarms that have been triggered or "No" (or 0) for alarms that have not been triggered. If desired, the /AS command line can also include an optional alarm argument that will cause the unit to display the status of one individual alarm as shown in the table below:

Alarm Name	Alarm Argument
Over Temperature (Initial)	OTI
Over Temperature (Critical)	OTC
Open Circuit Breaker	CBO
Ping No Answer	PNA
Serial Port Invalid Access Lockout	LO
Power Cycle (Cold Boot)	CB
Lost Voltage (Line In)	VL
No Dialtone	ND
Emergency Shutoff	ES

Availability: Administrator

Format: **`/AS [alarm]`** **[Enter]**

Where **`alarm`** is an optional argument, which can be used to display the status of an individual alarm as shown in the table above.

/J Display Site ID / Unit Information

Displays the user-defined Site I.D. message. If the optional asterisk (*) argument is included in the command line, the command will also show model numbers, serial number, software versions and other information for the RPC unit.

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/J [*]`** **[Enter]**

Where **`*`** (asterisk) is an optional command argument, that is used to display the model number, software version and other information for the RPC unit.

17.3.2. Control Commands

/X Exit Command Mode

Exits command mode. When issued at the Network Port, also ends the Telnet session.

> **Note:** *If the /X command is invoked from within a configuration menu, recently defined parameters may not be saved. In order to make certain that parameters are saved, always press the **[Esc]** key to exit from all configuration menus and then wait until "Saving Configuration" message has been displayed and the cursor has returned to the command prompt before issuing the /X command.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/X`** **[Enter]**

/BOOT Initiate Boot Cycle

Initiates a boot cycle at the selected circuit(s) or Circuit Group(s). When a Boot cycle is performed, the RPC will first switch the selected circuit(s) Off, then pause for the user-defined Boot/Sequence Delay Period, then switch the circuit(s) back on. The /BOOT command can also be entered as /BO.

Notes:

- *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all RPC circuits and Circuit Groups. When this command is invoked in User Mode, it can only be applied to the circuits and/or Circuit Groups that have been enabled for the account.*
- *When the /BOOT command is used to reboot more than one plug, the Boot/Sequence Delay Periods will be applied as described in Section 5.7.*

Availability: Administrator, SuperUser, User

Format: **`/BOOT <s>[,Y]`** **[Enter]** or **`/BO <s>`** **[Enter]**

Where:

`s`	The number or name of the circuit(s) or Circuit Group(s) that you intend to boot. To apply the command to several circuits, enter a plus sign (+) between each circuit number. To apply the command to a range of circuits, enter the numbers for the first and last circuits in the range, separated by a colon character (:). To apply the command to all circuits allowed by your account, enter an asterisk character (*).
`,Y`	(Optional) Suppresses the command confirmation prompt.

Example:

Assume that your account allows access to Circuit A2 and Circuit A3. To initiate a boot cycle at Circuits A2 and A3, without displaying the optional command confirmation prompt, invoke either of the following command lines:

`/BOOT A2+A3,Y` **[Enter]** or **`/BO A2+A3,Y`** **[Enter]**

/ON Switch Circuit(s) ON

Switches selected circuits(s) or Circuit Group(s) On, as described in Section 9.2.2. When the /ON command is used to switch more than one circuit, Boot/Sequence Delay Period will be applied as described in Section 5.7.

Notes:

- *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all RPC circuits and Circuit Groups. When this command is invoked in User Mode, it can only be applied to the circuits and/or Circuit Groups that have been enabled for the account.*
- *When the /BOOT command is used to reboot more than one plug, the Boot/Sequence Delay Periods will be applied as described in Section 5.7.*

Availability: Administrator, SuperUser, User

Format: **`/ON <s>[,Y]`** **[Enter]**

Where:

`s` The number or name of the circuit(s) or Circuit Group(s) that you intend to Switch On. To apply the command to several circuits, enter a plus sign (+) between each circuit number. To apply the command to a range of circuits, enter the numbers for the first and last circuits in the range, separated by a colon character (:). To apply the command to all circuits allowed by your account, enter an asterisk character (**`*`**).

`,Y` (Optional) Suppresses the command confirmation prompt.

Example:

Assume that your account allows access to Circuit A2 and Circuit A3. To switch Circuits A2 and A3 On, without displaying the optional command confirmation prompt, invoke following command line:

`/ON A2+A3,Y` **[Enter]**

/OFF Switch Circuit(s) OFF

Switches selected circuits(s) or Circuit Group(s) Off, as described in Section 9.2.2. When the /OFF command is used to switch more than one circuit, Boot/Sequence Delay Period will be applied as described in Section 5.7. The /OFF command can also be entered as /OF.

> **Note:** *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all RPC circuits and Circuit Groups. When invoked in User Mode, the command can only be applied to the circuits and/or Circuit Groups that are enabled for the account.*

Availability: Administrator, SuperUser, User

Format: **`/OFF <s>[,Y]`** **[Enter]** or **`/OF <s>[,Y]`** **[Enter]**

Where:

`s` The number or name of the circuit(s) or Circuit Group(s) that you intend to Switch Off. To apply the command to several circuits, enter a plus sign (+) between each circuit number. To apply the command to a range of circuits, enter the numbers for the first and last circuits in the range, separated by a colon character (:). To apply the command to all circuits allowed by your account, enter an asterisk character (*).

`,Y` (Optional) Suppresses the command confirmation prompt.

Example:
Assume that your account allows access to Circuit A2 and Circuit A3. To switch Circuits A2 and A3 on your local RPC unit Off, without displaying the optional command confirmation prompt, invoke either of the following command lines:

`/OFF A2+A3,Y` **[Enter]** or **`/OF A2+A3,Y`** **[Enter]**

/DPL Set All Circuits to Default States

Sets all switched circuits to their user-defined default state. For information on setting circuit defaults, please refer to Section 5.7.

> **Note:** *When this command is invoked in Administrator Mode or SuperUser Mode, it will be applied to all RPC circuits. When invoked in User Mode, the command will only be applied to the circuits that are allowed by the account.*

Availability: Administrator, SuperUser, User

Format: **`/DPL[,Y]`** **[Enter]**

Where ,Y is an optional command argument, which can be included to suppress the command confirmation prompt.

/TELNET Outbound Telnet

Creates an outbound Telnet connection.

Notes:

- *In order for the /TELNET command to function, Telnet/SSH and Outbound Service Access must be enabled for your user account as described in Section 5.5. In addition, Telnet Access and Outbound Access must also be enabled via the Network Parameters menu, as described in Section 5.9.2.*
- *If you have logged in via the Network Port, the /TELNET command will not function.*

Availability: Administrator, SuperUser, User

Format: **`/TELNET <ip> [port] [raw]`** **[Enter]**

Where:

`ip`	Is the target IP address. The IP Address can be entered in either IPv4 or IPv6 format.
`port`	Is an optional argument which can be included to indicate the target port at the IP address.
`raw`	Is an optional argument which can be included to indicate a raw socket connection. In order to create a raw socket connection, the command line must end with the text "**`raw`**".

/SSH Outbound SSH

Creates an outbound SSH connection.

Notes:

- *In order for the /SSH command to function, Telnet/SSH and Outbound Service Access must be enabled for your user account as described in Section 5.5. In addition, SSH Access and Outbound Access must also be enabled via the Network Parameters menu, as described in Section 5.9.2.*
- *If you have logged in via the Network Port, the /SSH command will not function.*

Availability: Administrator, SuperUser, User

Format: **`/SSH <ip> -l <username>`** **[Enter]**

Where:

`ip`	Is the target IP address. The IP Address can be entered in either IPv4 or IPv6 format.
`-l`	(Lowercase letter "L") Indicates that the next argument will be the log on name.
`username`	Is the username that you wish to use to log in to the target device.

/C Connect to Serial Port

When the RJ-45 Console Port has been configured as a Normal Mode Port as described in Section 5.8, the /C command can be used to create a connection between the Network port and the Console Port.

Notes:

- *User level accounts can only connect to the Console Port when serial port access is specifically permitted by the account.*
- *To terminate a port connection, either type* **^x** *(**[Ctrl]** plus **[X]**) or invoke the currently defined disconnect sequence.*

Availability: Administrator, SuperUser, User

Format: `/C 1` **[Enter]**

/U Send Parameters to File

Sends all RPC configuration parameters to an ASCII text file as described in Section 15. This allows you to back up the configuration of your RPC unit.

Availability: Administrator

Format: `/U` **[Enter]**

/K Send SSH Key

Instructs the RPC to provide you with a public SSH key for validation purposes. This public key can then be provided to your SSH client, in order to prevent the SSH client from warning you that the user is not recognized when you attempt to create an SSH connection. For more information, please refer to Section 10.

Availability: Administrator

Format: `/K k` **[Enter]**

Where k is a required argument, which indicates the key type. The k argument provides the following options: 1 (SSH1), 2 (SSH2 RSA), 3 (SSH2 DSA.)

/UL Unlock Port (Invalid Access Lockout)

Manually cancels the RPC's Invalid Access Lockout feature. Normally, when a series of failed login attempts are detected, the Invalid Access Lockout feature can shut down the network port for a user specified time period in order to prevent further access attempts. When the /UL command is invoked, the RPC will immediately unlock all network ports that are currently in the locked state.

Availability: Administrator

Format: `/UL` **[Enter]**

Response: Unlocks the RPC's RS232 Console Port.

17.3.3. Configuration Commands

/F Set System Parameters

Displays a menu which is used to define the Site ID message, create user accounts, set the system clock, enter the unit serial number and configure and enable the Invalid Access Lockout feature. Note that all functions provided by the /F command are also available via the Web Browser Interface. For more information, please refer to Section 5.3.

Availability: Administrator
Format: `/F` **[Enter]**

/P Set Serial Port Parameters

Displays a menu that is used to select options and parameters for the RPC's serial Console Port. Note that all functions provided by the /P command are also available via the Web Browser Interface. Section 5.8 describes the procedure for defining serial port parameters for the Console Port.

Availability: Administrator
Format: `/P` **[Enter]**

/PL Set Circuit Parameters

Displays a menu that is used to select options and parameters for the RPC's switched circuits. Note that all functions provided by the /PL command are also available via the Web Browser Interface. Section 5.7 describes the procedure for defining circuit parameters.

Availability: Administrator
Format: `/PL` **[Enter]**

/G Circuit Group Parameters

Displays a menu that is used to View, Add, Modify or Delete Circuit Groups. For more information on Circuit Groups, please refer to Section 5.6.

Availability: Administrator
Format: `/G` **[Enter]**

/N Network Port Parameters - IPv4

Displays a menu which is used to select IPv4 parameters for the Network Port. Note that all of the functions provided by the /N command are also available via the Web Browser Interface. For more information, please refer to Section 5.9.

Availability: Administrator
Format: **`/N`** **[Enter]**

/N6 Network Port Parameters - IPv6

Displays a menu which is used to select IPv6 parameters for the Network Port. Note that all functions provided by the /N6 command are also available via the Web Browser Interface. For more information, please refer to Section 5.9.

Availability: Administrator
Format: **`/N6`** **[Enter]**

/RB Reboot Options

Displays a menu that is used to configure Scheduled Reboots and Ping-No-Answer Reboots. Scheduled Reboots allow the RPC to be rebooted on a regular basis, according to a user defined schedule. Ping-No-Answer Reboots allow the RPC to automatically reboot user-designated circuits when a user-specified IP address does not respond to a Ping command. For more information on Reboot options, please refer to Section 6.

> **Note:** *If desired, the Ping-No-Answer Reboot function can also be configured to send email notification whenever a Ping-No-Answer Reboot is generated. For more information, please refer to Section 7.4.*

Availability: Administrator
Format: **`/RB`** **[Enter]**

/AC Alarm Configuration Parameters

Displays a menu that is used to configure and enable the RPC's various alarm functions. For more information on Alarm Configuration, please refer to Section 7.

Availability: Administrator
Format: **`/AC`** **[Enter]**

/I Reboot System (Default)

Reinitializes the RPC unit and offers the option to keep user-defined parameters or reset to default parameters. As described in Section 5.10.1, the /I command can also be used to restore the unit to previously saved parameters. When the /I command is invoked, the unit will offer the following reboot options:

- Reboot Only (Do NOT default parameters)
- Reboot & Default (Keep IP Parameters & SSH Keys)
- Reboot & Default (Default ALL parameters)
- Reboot & Restore Last Known Working Configuration

Availability: Administrator, SuperUser

Format: **`/I`** **[Enter]**

/UF Upgrade Firmware

When new versions of the RPC firmware become available, this command is used to update existing firmware as described in Section 16.

> **Note:** *When a firmware upgrade is performed, it will take about 15 minutes to upgrade the RPC unit.*

Availability: Administrator

Format: **`/UF`** **[Enter]**

/TEST Test Network Parameters

Displays a menu which is used to test configuration of the Syslog and SNMP Trap functions and can also be used to invoke a Ping Command. For more information, please refer to Section 11.2 and Section 12.2.

Notes:

- *In order for the ping command to function with domain names, Domain Name Server parameters must be defined as described in Section 5.9.5.*
- *The Test Menu's Ping command is not effected by the status of the Network Parameters Menu's Ping Access function.*

Availability: Administrator

Format: **`/TEST`** **[Enter]**

Appendix A. Specifications

A.1. RPC-4850 Series Units

Power Input / Output:

- **Voltage:** -48 VDC
  - **RPC-4850-48V Units:** -18 to -72 VDC
  - **RPC-4850-24V Units:** 18 to 72 VDC
- **DC Inputs:**
  - Two (2); Bus A and/or Bus B, 50-Amps Maximum per Bus.
  - **Connector:** Terminal Block; #10 Screws
- **DC Output Circuits:** Eight (8)
  - **Connectors:** Terminal Block, #8 Screws
  - **Load:** 15 Amps Max per Circuit (Total for Circuits One through Eight not to exceed 50 Amps.)

Control Ports:

- **Network Port:** Ethernet, 10/100Base-T
- **Console / Modem Port:** DB9M, RS232C, DTE
- **RS232 Coding:** Serial ASCII, 7/8 Bits, No Parity, 300 bps - 115 Kbps.

Physical / Environmental:

- **LED Indicators:** ON, RDY, RXD, Circuit On (1 - 8)
- **Size:**
  - **Height:** 3.5" (8.9 cm) (2 RU)
  - **Width:** 19.0" (48.3 cm) Standard Rack
  - **Depth:** 9.5" (24.1 cm)
- **Shipping Weight:** 13 Lbs. (5.9 Kg)
- **Operating Temperature:** 32°F to 149°F (0°C to 65°C)
- **Humidity:** 10 - 90% RH

A.2. RPC-40L8A4 Series Units

Power Input / Output:

- **Voltage:** -48 VDC
  - **RPC-40L8A4-48 Units:** 18 to 72 VDC
  - **RPC-40L8A4-24 Units:** 18 to 75 VDC
  - **RPC-40L8A4-12 Units:** 9 to 36 VDC
- **DC Inputs:** Two (2) Bus A and Bus B, 40 Amps Maximum per Bus.
  - **Connector:** Terminal Block, #10 Screws
- **DC Output Circuits:** Eight (8), Two Blocks of Four (4) Eurostyle Connectors
  - **Load:** 10 Amps Max per Circuit (Total for each branch not to exceed 40 Amps.)
- **Alarm Ports:** Four (4) Two Pin Eurostyle Connectors

Control Ports:

- **Network Port:** Ethernet, 10/100Base-T
- **Console / Modem Port:** DB9M, RS232C, DTE
- **RS232 Coding:** Serial ASCII, 7/8 Bits, No Parity, 300 bps - 115 Kbps.

Physical / Environmental:

- **LED Indicators:** ON, RDY, RXD, Circuit On (1 - 8)
- **Size:**
  - **Height:** 1.74" (4.4 cm) (1 RU)
  - **Width:** 19.0" (48.3 cm) Standard Rack
  - **Depth:** 9.5" (24.1 cm)
- **Shipping Weight:** 10 Lbs. (4.5 Kg)
- **Operating Temperature:** 32°F to 149°F (0°C to 65°C)
- **Humidity:** 10 - 90% RH

Appendix B. Interface Descriptions

B.1. RS232 Console Port - RPC-4850 Series Units

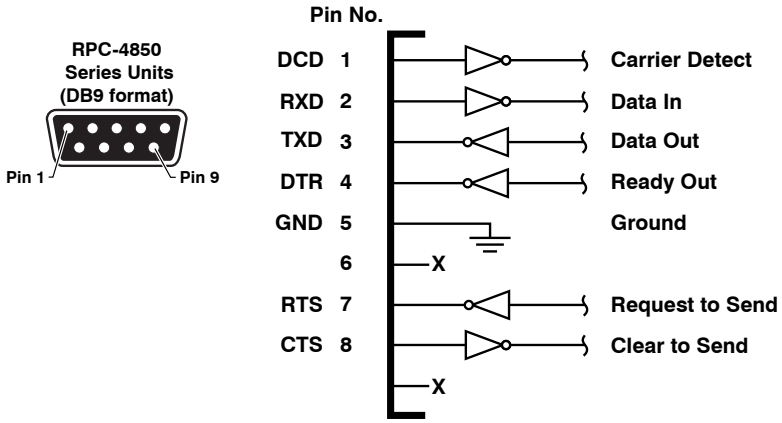

Figure B.1: RS232 Console Port Interface - RPC-4850 Series Units

B.2. RS232 Console Port - RPC-40L8A4 Series Units

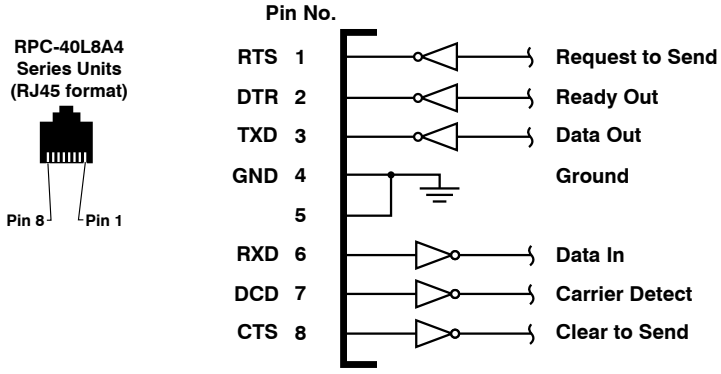

Figure B.2: RS232 Console Port Interface - RPC-40L8A4 Series Units

Appendix C. Customer Service

Customer Service hours are from 8:00 AM to 5:00 PM, PST, Monday through Friday. When calling, please be prepared to give the name and make of the unit, its serial number and a description of its symptoms. If the unit should need to be returned for factory repair it must be accompanied by a Return Authorization number from Customer Service.

WTI Customer Service
5 Sterling
Irvine, California 92618

Local Phone: (949) 586-9950
Toll Free Service Line: 1-888-280-7227
Service Fax: (949) 583-9514

Email: service@wti.com

Trademark and Copyright Information

WTI and Western Telematic are trademarks of Western Telematic Inc.. All other product names mentioned in this publication are trademarks or registered trademarks of their respective companies.

Information and descriptions contained herein are property of Western Telematic, Inc.. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Western Telematic Inc..

© Copyright Western Telematic Inc., 2014.

August, 2014
Part Number: 13532, Revision: D

Trademarks and Copyrights Used in this Manual

Cisco and EnergyWise are registered trademarks of Cisco Systems, Inc.

Hyperterminal is a registered trademark of the Microsoft Corporation. Portions copyright Hilgraeve, Inc.

ProComm is a trademark of Datastorm Technologies, Inc™.

Teraterm is a copyright of Ayera Technologies, Inc.

BlackBerry is a registered trademark of Research In Motion Limited.

JavaScript is a trademark of Sun Microsystems, Inc.

Telnet is a trademark of Telnet Communications, Inc.

All other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.